

PRODISCOVER[®]

Computer Forensics Family

User Manual

Copyright

© 2003-2006 Technology Pathways, LLC. All rights reserved. This manual, as well as the software described in it, are furnished under license and may only be used in accordance with the terms of such license. The information furnished in this manual is for informational use only and is subject to change without notice. It should not be construed as a commitment, representation or warranty regarding the performance of the ProDiscover IR by Technology Pathways, LLC. Technology Pathways, LLC. assumes no responsibility for the consequences or any errors or inaccuracies in this manual.

Trademarks

ProDiscover® is a registered trademark of Technology Pathways, LLC. These and other graphics, logos, service marks, and trademarks of Technology Pathways, LLC may not be used without prior written consent of Technology Pathways, LLC. All other brand and product names are trademarks or registered marks of their respective holders.

Company names and dates used in examples herein are fictitious unless noted otherwise.

Printed in the USA.

Contacting Technology Pathways, LLC.

Corporate Headquarters

Address: Technology Pathways, LLC.
703 First Street
Coronado, California, 92118
USA

Telephone: (619) 435-0906

Fax: (619) 435-0465

World Wide Web: www.TechPathways.com

Office Hours: Monday to Friday
9 am to 5 pm Pacific Standard Time

Sales

Phone: (888) 894.5500

**International
(including Canada):** (619) 435-0906

Fax: (619) 435-0465

Email: sales@TechPathways.com

Technical Support

Technical support for ProDiscover is provided to all registered customers via a variety of means. Before contacting technical support, users should prepare to provide the following information.

- Locate your product authorization number from the front of the quick start guide.
- Determine your operating system and version.
- Find the version of ProDiscover in the About box.

Phone:	(619) 435-0906
Fax:	(619) 435-0465
Email:	support@TechPathways.com
Office hours:	Monday to Friday 9am to 5pm Pacific Standard Time
24-hour World Wide Web support:	www.TechPathways.com

ProDiscover Community Forum

The new ProDiscover Community Forum designed to serve as knowledge management and collaboration Lists for ProDiscover Users is now online. The new Web based forums are available through a link from the Technology Pathways Web site "Support" tab at: <http://www.techpathways.com/DesktopDefault.aspx?tabindex=7&tabid=11> or directly from: <http://toorcon.techpathways.com/CS/forums/>

NOTE: Support for ProDiscover Basic edition is provided only via the online forums.

Table of Contents

WELCOME TO PRODISCOVER ®	1
GETTING STARTED	3
System requirements	3
Hardware.....	3
Software.....	3
Installing ProDiscover	3
Important Driver Installations.....	3
Licensing and Activating ProDiscover	4
Starting ProDiscover.....	5
About ActivePerl.....	5
Basic features of ProDiscover	6
Basic steps to use ProDiscover	7
Customizing ProDiscover.....	7
Status Bar	7
Tool Bar	7
Startup Dialog	7
Preferences	7
Getting Help	9
ProDiscover Support	9
Active Perl Support.....	9
MOVING AROUND IN PRODISCOVER	11
Main Window	11
Data View Area Buttons	11
First	12
Go	12
Last.....	12
Next.....	12
Back.....	12
Tree View Area Items.....	12
Button Bar	13
File Menu	14
Network Menu	14
Action Menu	14
View Menu	15
Tools Menu	15
IR Menu (ProDiscover IR Edition only)	16
Help Menu	16

USING PRODISCOVER.....	17
Creating a New Project	17
Save a Project.....	17
Preview a directly connected evidence drive.....	18
Conducting Live Preview of a Remote Disk	20
Capture an image of an attached drive.....	21
Capturing Physical Memory.....	22
Add an image file to a project	26
Add a UNIX "dd" image file to a project	28
Copy a directly connected drive to another directly connected drive	30
Restore an Image to directly connected drive	31
Copy Selected Files	31
List detail information about image files associated with a project	32
View the contents of a directly connected disk as files.....	32
View the contents of a disk, or image file as clusters	32
Viewing the Windows Event Logs.....	33
View Windows Registry	33
Search the Windows Registry	35
View Graphic Files in Gallery View	39
Adding Thumbnail Images to Report for Graphic Evidence	40
View Image EXIF Meta Data	40
Recover a Deleted File	42
Search for key words in image file or disk.....	43
Extracting Internet History	45
Creating Hash Database Files	46
Comparing HashKeeper hash sets	47
To compare hash sets to a directory and all contents recursively:	47
To compare hash sets to a single file:	48
Match File Signatures and File Extensions	49
Detecting file systems within the HPA.....	50
Recover a group of clusters	53
Detecting Disk or Image Installed OS	54
Cross Reference File Cluster Locations.....	56
To find a list of specific clusters in which a file is written:	56
To find the file associated with a specific cluster:	57
Determining and Cross Referencing a File's Cluster Locations.....	58
Flagging or Bookmarking Evidence of Interest.....	58
Adding and Editing Comments to Evidence of Interest	60
Adding Subsets of Data as Evidence of Interest	61

USING PRODISCOVER REMOTE AGENT 63

Network Imaging & Analysis of Live Systems (ProDiscover Investigator and IR Version)	63
PDServer Security.....	64
Encryption.....	64
Secure Communication Protocol.....	64
Password Protection.....	64
Password Lockout	65
Write Protected Trusted Binaries.....	65
Other Safeguards.....	65
Creating a Windows PDServer Disk (ProDiscover IR & Investigator Version)	65
ProDiscover Investigator Version.....	65
Creating and Running the Sun Remote Agent	65
Creating a Linux PDServer Disk	66
Creating a PDServer Linux Boot Disk	66
PDServer in Stealth Mode (ProDiscover IR & Investigator Version)	66
Install Stealth Mode (Automated Installation)	66
Install Stealth Mode (Manual Installation).....	67
Switch to Stealth Mode.....	68
PDServer Command Line Options	68
Stealth Only Remote Agent (ProDiscover Investigator and Incident Response only) .	69
Using the PDServer Linux Boot Disk	69
ProDiscover & PDServer Remote Agent Firewall Configuration.....	70
Components of a Secured Network System.....	70
ProDiscover and Firewalls.....	70
Firewall Limitations	70
Security and Policy Concerns	71
PDServer™ Remote Installation and Removal Scripts	72
Troubleshooting PDServer Connection Problems.....	75
Getting Started	75
Using “PING” and “TRACEROUTE” to Diagnose Problems	76
Using Ping in DOS (Command Prompt)	76
Using Traceroute in DOS (Command Prompt)	76
ProDiscover Setup and Communications Flow	77
Remote Push through the ProDiscover GUI.....	78
Windows XP Firewalling Guide.....	79
Windows 2000 Packet Filtering.....	83
Push Checklist	86
Connection Checklist.....	87

INTRODUCTION TO THE PROSCRIPT API AND PERL 89

Writing and Debugging ProScripts	89
--	----

ADVANCED TIPS AND TRICKS	93
Deleted Files.	93
ATA Hardware Protected Areas (HPA).	93
Alternate Data Streams in Windows NT/2000/XP.	94
System \$ meta files in Windows NT/2000/XP.....	94
EXIF Meta Data found in JPG and TIFF graphics files.....	95
Timeline Analysis Techniques.	95
APPENDIX A: PRODISCOVER COMMANDS	97
Tree View Commands.....	97
Report.....	97
Add Capture & Add Image	98
Add Image.....	98
Add Disk.....	99
Remove.....	100
Content View Image.....	101
Content View Disk.....	101
Cluster View	101
Cluster View of Physical Drive.....	102
Cluster View of Drive Partition.....	103
Registry Viewer	103
EventLog Viewer	103
Internet History Viewer.....	104
View Log.....	104
Search.....	105
File Menu Commands.....	108
New Project	108
Open Project.....	108
Open Image	108
Save Project	108
Save As	108
Preferences	109
Print Setup	114
Print Report.....	115
Exit	115
Network Menu Commands	116
Connect To	116
Disconnect.....	116
Encryption.....	117
Release Remote Client.....	117
Action Menu Commands	118
Capture Image	118

Add Capture & Add Image	120
Add Image	120
Add Disk	121
Search –	122
Stop Search	124
Clear Report Evidence of Interest	124
Clear Report Search Results	124
Clear Report File Signature Mismatch	124
Clear Report OS Info	124
Clear Report Clusters of Interest	125
Clear Report Unseen Processes	125
Clear Report Registry Keys of Interest	125
Clear Report Process List	125
Clear Report System State	125
Clear Report Ports List	125
Clear Report All	125
Clear Recent Projects List	125
Compress	125
UnCompress	126
Export	126
Verify Image Checksum	127
Disk Inventory	127
OS Info	127
Export Evidence of Interest	128
Create report thumbnails	128
View Menu Commands	129
Report	129
Content View Image	129
Content View Disk	130
Cluster View	130
Cluster View of Physical Drive	130
Cluster View of Drive Partition	131
View Log File	132
Startup Dialog	132
Tool Bar	132
Status Bar	132
Gallery View	132
Tools Menu Commands	135
Secure Wipe	135
Copy Disk	135
Copy Selected Files	135
Copy Selected Clusters	136
Filter by Hash Set	137
Batch Calculate Hashing	137

Signature Matching	137
Scan HPA.....	138
Image Conversion Tools	138
Convert Project Format	140
Create remote server disk.....	140
IR Menu Commands (ProDiscover IR Edition only).....	141
Find Unseen Processes	141
Find Unseen Files.....	141
Create Baseline	143
Compare Baseline.....	144
Find Suspect Files	144
Get Process List	146
Get System State.....	146
Open/Connected IP Ports	148
APPENDIX B: UTILIZING BOOLEAN LOGIC IN KEYWORD SEARCH	
TERMS	149
Basic Boolean Search Strategy	150
APPENDIX C: INCIDENT RESPONSE WITH PRODISCOVER IR	151
APPENDIX D: BASIC COMPUTER FORENSICS	159
What is Computer Forensics.....	159
Stay Informed	159
Standard Practices & Documentation	159
Maintain Chain of Custody	160
Physical Storage	160
Computer Shutdown.....	160
Imaging Evidence Drives	160
Evidence Examination	161
References	161
Agencies, Contacts & Resources.....	162
List Servers	162
APPENDIX E: END-USER LICENSE AGREEMENT AND PRODUCT	
LICENSING	163
Software Licence and Copy Protection.....	163
End-User License Agreement	163
INDEX.....	165

PRODISCOVER[®]

■■■■

Computer Forensics Family

Welcome to ProDiscover[®]

The ProDiscover Family of computer security tools enables systems administrators, consultants, and investigators find the data they need on a computer disc. Whether you suspect your system has been hacked or are looking for discoverable evidence in a civil proceeding or criminal investigation, ProDiscover will make your job easier, improve your productivity, and preserve the data needed for any legal proceedings. Designed to the National Institute of Standards Disk Imaging Tool Specification 3.1.6, the ProDiscover Family provides affordable solutions for:

Incident Response

Quickly and positively identify intrusions to your systems without taking your system down. Get any corrupted system back on-line quickly and gather the evidence needed to prosecute an intruder.

Corporate Policy Compliance Investigation

Check for policy violations or conduct internal investigations remotely through your company's network.

E-discovery

Improve your productivity and insure compliance in any civil discovery action. Quickly search large data sets and find the documents you need. Preserve critical "last accessed" metadata and document your results.

Computer Forensics

Find all the data, even in hidden HPA section, Alternate Data Streams or slack space. Create hash signatures for all files and compare them to the information from the National Drug Intelligence "Hashkeeper" database. Automatically generate reports and "evidentiary quality" information that may be used court.

The ProDiscover Family of computer security tools include:

ProDiscover for Windows

Offering forensics examiners a completely integrated Windows[™] application for the collection, analysis, management and reporting of computer disk evidence at an affordable price. ProDiscover for Windows supports all Windows based file systems including FAT 12/16/32 and NTFS Dynamic disks.

ProDiscover Forensics

ProDiscover Forensics edition provides all the capabilities as ProDiscover for Windows and also includes all additionally supported file systems such as SUN Solaris UFS and Linux Ext2/3.

ProDiscover Investigator

ProDiscover Investigator takes the ProDiscover Forensics workstation product and turns it into a fully client server application allowing disk preview, imaging and analysis over any TCP/IP network.

ProDiscover Incident Response

Includes all the features of ProDiscover Investigator plus contains advanced tools for Incident Response and network preview, imaging & analysis.

Please note that all versions of ProDiscover are forensics products which take a least-intrusive approach to working with disk evidence. ProDiscover implements its own read-only file system viewers and does not rely on the underlying operating file system for analysis of evidence.

When ProDiscover is launched, the user is asked to perform one of the following tasks:

[New Project](#) - Displays the new project tab (shown below) and creates a new project, as specified by the user, in the main window. New project option prompts the user for a project number, project name and description and creates a template report in the work area.

[Open Project](#) - Displays the open project tab (shown below) and opens the project specified by the user in the main window. This opens a file dialog with default extension set to *.dft the default project file extension. When the user selects a valid project file, this loads the file data in the work area.

[Open Recent Project](#) - Displays the recent project tab (shown below), and displays the recently opened project files.

By default project files are saved to the ProDiscover installation directory with the file extension (*.dft). Project files are kept in XML format allowing users to parse the file with other applications to create custom reports from a variety of applications. The current ProDiscover XML Schema can be found in the default application installation directory.



Getting started

System requirements

Hardware

The minimum hardware requirements are:

CPU:	1.2 Ghz Pentium III or later
Memory:	256MB or greater (512 MB Recommended)
Available disk space:	500MB (a large amount of temporary space for viewing and hashing evidence files)
Media:	CD-ROM or DVD-ROM Drive
Monitor:	VGA or High Resolution Monitor
Input and Control:	Keyboard & Mouse or compatible pointing device

Software

The minimum software requirements are:

Operating System:	Windows 2000/2003/XP
Other software:	ActiveState Perl (Included) Desired file viewers

Installing ProDiscover

The ProDiscover CD contains an automated setup program that will guide you through the installation process outlined below:

1. Close all programs.
2. Insert the CD labeled **ProDiscover** into your CD-ROM drive.
3. From the **Start** menu, select **Run**.
4. Type **D:\setup** (substitute the appropriate letter of your CD-ROM drive for D).
5. Follow the instructions on the screen.
6. Once installed, ProDiscover must be activated with the client activator. Instructions for activating ProDiscover are included in the quick start guide.

By default, ProDiscover is installed in **C:\Program Files\Technology Pathways\ProDiscover**.

Important Driver Installations

Beginning with ProDiscover 1.54 a Windows device driver is included for detection and analysis of the Hardware Protected Area on ATA drives. After installing ProDiscover for the first time, install the paremove.sys device driver as instructed below. Note: For users who desire not to install the driver, ProDiscover will function normally without any HPA support. The HPA driver is not compatible on systems running Windows NT 4.0.

Windows 2000

1. Click Start.
2. Choose Settings.
3. Click on the Control Panel.
4. Choose Add/Remove Hardware.
5. Click Next for the Welcome dialog .
6. Choose Add/Troubleshoot a device option and click Next.

7. Windows will search for the new hardware and proceed to the next screen.
8. In the Choose a hardware device screen, choose "Add a new Device" and click Next
9. In the Find New Hardware, choose "No, I want to select the hardware from the list" option and click Next.
10. In the Hardware type, choose Other devices and click Next.
11. Windows will show all the device drivers' information in the Select a Device driver screen.
12. Click Have Disk button.
13. Using the browse button locate and choose the paremove.inf file contained in your ProDiscover installation directory's "Driver" subdirectory.
14. Select the Technology Pathways PAREmove Driver from the list and click Next.
15. Just click Next for the Start Hardware Installation screen.
16. Choose Finish and restart the computer.

Windows XP

1. Choose "Add Hardware" from the control panel
2. Choose "Next"
3. Select "Yes, I have already connected the hardware"
4. Choose "Next"
5. Choose "Add a new hardware device" from the bottom of the installed hardware windows.
6. Choose "Next"
7. Choose "Install the hardware that I manually select from a list"
8. Choose "Next"
9. Double-Click on "Show All Devices"
10. Choose "Next"
11. Choose "Have Disk..."
12. Using the browse button locate and choose the paremove.inf file contained in your ProDiscover installation directory's "Driver" subdirectory.
13. Choose "Open"
14. Choose "OK"

Licensing and Activating ProDiscover

Each copy of ProDiscover is licensed for one concurrent use and may be installed on up to three workstations. For detailed information on authorized use of ProDiscover please consult your specific product license agreement.

A product license activation file will be emailed to you by Technology Pathways support. The ProDiscover license file is a single file with the extension *.VPL for instance the license file for ProDiscover Investigator is "ProDiscoverIN.VPL".

Once you have installed your copy of ProDiscover copy license activation file to the ProDiscover installation directory. The default installation directory is:

C:\Program Files\Technology Pathways\ProDiscover\

The ProDiscover license file activates your product and should be backed up for future use and installations.

Your product is now licensed and activated.

Starting ProDiscover

Once installation is complete, you will see a ProDiscover icon on your desktop.

To start ProDiscover

- Click the **ProDiscover** icon.
- OR
- From the **Start** menu, select **Programs - ProDiscover**.

About ActivePerl

Many versions of ProDiscover include the ActivePerl distribution from ActiveState along with the ProScript API which is exposed to the included Active Perl distribution for user scripting and automation. ActivePerl is the up-to-date, quality-assured Perl binary distribution from ActiveState. Current releases, and other professional tools for open source language developers are available at

<http://www.ActiveState.com>.

The ActiveState Repository has a large collection of modules and extensions in binary packages that are easy to install and use. To view and install these packages, use the Perl Package Manager (PPM) which is included with ActivePerl.

Basic features of ProDiscover

Key features of ProDiscover include the following:

- ☒ Designed specifically to meet requirements set in October 2001 by NIST (National Institute of Science and Technology) Disk Imaging Tool Specification 3.1.6
- ☒ Supports non-destructive direct disk analysis
- ☒ Create compressed image files to work from
- ☒ Create and Analyze Unix "dd" images of supported file systems
- ☒ The ability to image and conduct live analysis of disks over any high speed TCP/IP network (except ProDiscover *for Windows* and ProDiscover *Forensics*)
- ☒ Restore image files to disk
- ☒ Search and analyze media from all of the different Windows file systems, including FAT12, FAT16, FAT32, and all NTFS file systems including software RAID and dynamic disks
- ☒ Search and analyze media from Sun Solaris UFS, and Linux ext2/ext3 (except ProDiscover *for Windows*)
- ☒ Image Ram memory (except ProDiscover *for Windows* and ProDiscover *Forensics*)
- ☒ Capture Volatile System State information (ProDiscover *Incident Response* only)
- ☒ Displays Windows NT/2000™ Alternate Data Streams
- ☒ Bit stream copy disk to new disk (including ATA Protected Areas)
- ☒ Create MD5, SHA1, or SHA256 hash of images and files
- ☒ Utilize Perl Scripts to automate key processes (except for ProDiscover *for Windows*)
- ☒ Compare HashKeeper checksums to disk contents
- ☒ Cross-reference file clusters between content-view (files) and cluster-view
- ☒ Detect operating system installed
- ☒ Access project file in XML format
- ☒ Analyze file header signatures to file extensions and detect mismatches
- ☒ Extract and view EXIF meta data from JPEG and TIFF graphics files
- ☒ View Windows Registry and add any registry key to report as evidence of interest
- ☒ View graphics thumbnails in gallery view format, add graphic thumbnail to report
- ☒ I/O error reporting
- ☒ Automatic report generation
- ☒ Add comments to report for evidence of interest
- ☒ Bates number and batch transfer evidence of interest
- ☒ Extensive search capability
- ☒ Recover deleted files contained in slack space
- ☒ Secure Wipe Disk
- ☒ Create and compare baseline hash signatures sets to detect any file changes (ProDiscover *Incident Response* and ProDiscover *Suite* only)
- ☒ Find Unseen files and processes on Windows systems (ProDiscover *Incident Response* and ProDiscover *Suite* only)
- ☒ Online Help

Basic steps to use ProDiscover

ProDiscover is designed to be a single application allowing forensics examiners to collect, analyze, manage and report on computer disk evidence. Essentially, ProDiscover simplifies computer forensics case management.

The following high-level, overview of steps a user may take while using ProDiscover highlights how ProDiscover simplifies the computer forensics case management process.

1. Create a project.
2. Create Disk Images (optional).
3. Connect to remote PDServer over the network (optional).
4. Add Disks (local or over the network) directly to a project for evidence preview.
5. Add captured images to project (UNIX "dd" or ProDiscover format.)
6. Compare disk files to hashkeeper hash sets to filter out known operating system and application files.
7. Compare file headers and detect any file signature/extension mismatches.
8. Perform keyword searches.
9. Cross reference file cluster locations on disk.
10. Review file system contents.
11. Review unallocated clusters and disk slack.
12. Mark evidence of interest - marking files as "selected" calculates hash values for the file and adds the file's information to the ProDiscover report as "Evidence of Interest". Marking files as "selected" can operate recursively through sub-directories and even be accomplished automatically as a result of search operations.
13. Batch copy any evidence of interest to CD.
14. Review and edit report.
15. Export and print report.

Customizing ProDiscover

Users can customize ProDiscover to better suit their particular needs in several ways.

Status Bar

The Status Bar selection found in the View menu allows the user to add and remove the Status Bar from the main window. Users find this useful when analyzing evidence which requires the maximum amount of screen space possible.

Tool Bar

The Tool Bar (also known as the button bar) selection found in the View menu allows the user to add and remove the Tool Bar from the main window. Users find this useful when analyzing evidence which requires the maximum amount of screen space possible.

Startup Dialog

This option is enabled by default when the user has not checked the "Don't show this dialog in future" option from a new project, open project and recent project dialog. A check mark on the menu item indicates the dialog will not be shown.

Preferences

The preferences menu item found in the File menu launches the preferences dialog box allowing the user to set, or change their personal preferences in any of five areas; General, PDServer, Appearance, Time Zone, and EXIF.

General

The user may select the hashing algorithm utilized by ProDiscover as SHA1, SHA256, MD5 or None. While the SHA1, and SHA256 hashing algorithm is considered by some to be stronger than MD5,

there are currently more hash sets available in MD5. Rest assured that MD5 is a very secure method of hashing verification. Note that while you can freely change the hashing algorithm at any time when working with a physical disk during analysis, image files will only support the hashing algorithm selected during capture. The selected hashing algorithm will be displayed in the ProDiscover status bar for easy reference.

Selecting "None" as a hashing algorithm allows users to select large groups of files as evidence of interest without creating hashes. In cases where large groups of files are being recursively selected, this feature can save time. Once the user desires to add file hash values to the ProDiscover report they can change the preferences setting to the desired hashing algorithm, then use "Batch Calculate Hashing..." from the Tools menu to calculate hashes for all files marked "selected" (evidence of interest).

Users may enable warning dialogs that had been disabled earlier and turn on "Auto Verify Image Checksum" to automatically verify image checksums when loading a project or adding an image to a project. **Warning: Turning on "Auto Verify Image Checksum" will cause image addition and project loading to become very slow.**

ProDiscover uses a "Working Folder" to place temporary files in during operations such as generating hash values. By default the "Working Folder" is set to use the current users Documents and Settings temporary folder. Users may select any desired location as the ProDiscover "Working Folder".

PDServer

The Default Port number field in the Preferences dialog box allows users to change the default TCP/IP port number used for connecting to remote systems running PDServer for network imaging & analysis. Note that if the default port of 6518 is changed on the ProDiscover client the default port number will also need to be changed on the remote PDServer. Changing the default port number on the ProDiscover client and server is often helpful in traversing firewalls with inbound and outbound port filtering.

The "Server Time-out" setting tells ProDiscover how long to wait without receiving packets before attempting to reestablish communications with the PDServer Remote Agent. The "Auto Retries" setting tells ProDiscover how many times to automatically attempt to reestablish communications after a "Server Time-out" has occurred. Adjusting the PDServer "Auto Retries" and "Server Time-out" settings can be helpful for busy networks and Wide Area Networks.

Appearance

The appearance section of the preferences dialog box allows users to set the display color for many file types including files which are marked as the result of hash comparisons and file signature mismatch comparison. Users are additionally provided a facility to change the project report font to any installed system font.

In the "report images" section, users are given the ability to adjust settings relating to adding thumbnail images to the report for all graphics files which are selected as evidence of interest.

"Add thumbnail image to report for graphic files" (default unchecked) when checked will cause a thumbnail image to be created and added to the report for any graphic file which is selected as evidence of interest. Users who choose this option after graphic files have been added as evidence of interest can use the Action menu's "Create report thumbnails" option to add thumbnails to the report.

"Create thumbnails on load" (default unchecked) when checked causes ProDiscover to automatically add thumbnail images to the report when opened. Warning: for large reports, when many graphic files are selected as evidence of interest, this can cause significant delay while loading a project file.

Time Zone

Because the NTFS file system maintains time zone information with files, it is important for investigators to set the proper image or disk time zone information to ensure MAC (Modified, Accessed and Created) times are displayed as they would be on the target system. The time zone preferences dialog allows users to set the ProDiscover time for the disk or image being analyzed. Users can also set whether or not daylight savings time (European summertime) is/was in effect for the disk or image.

EXIF

Allows users to choose which EXIF meta data fields will be extracted from graphics files and added to the project report if the graphics file is selected as evidence of interest.

Users are given the ability to "Add All" EXIF meta field values to the report, "Remove All" EXIF meta fields from the report, or to individually select field by field for addition to the project report.

Getting Help

ProDiscover Support

There are various ways to get Help on ProDiscover:

Application Help - From the ProDiscover **Help** menu, select **Contents**.

User Training Manual - The official ProDiscover User training manual provided in Technology Pathways official training classes. Contact Technology Pathways for details and class availability.

Online Application Help - Contains an online version of the application help system.

Help on the Web – Visit the support section of our Web site where you can learn about the support options available to you.

User Communities – Visit the User Communities section of the Technology Pathways web site to exchange answers and ideas with other users.

Technical Support - Provided for registered users of ProDiscover, personal product support is available. See the front of this manual for contact information.

The new ProDiscover Community Forum designed to serve as knowledge management and collaboration Lists for ProDiscover Users is now online. The new Web based forums are available through a link from the Technology Pathways Web site "Support" tab at:

<http://www.techpathways.com/DesktopDefault.aspx?tabindex=7&tabid=11> or directly from:

<http://toorcon.techpathways.com/CS/forums/>

NOTE: Support for ProDiscover Basic edition is provided only via the online forums.

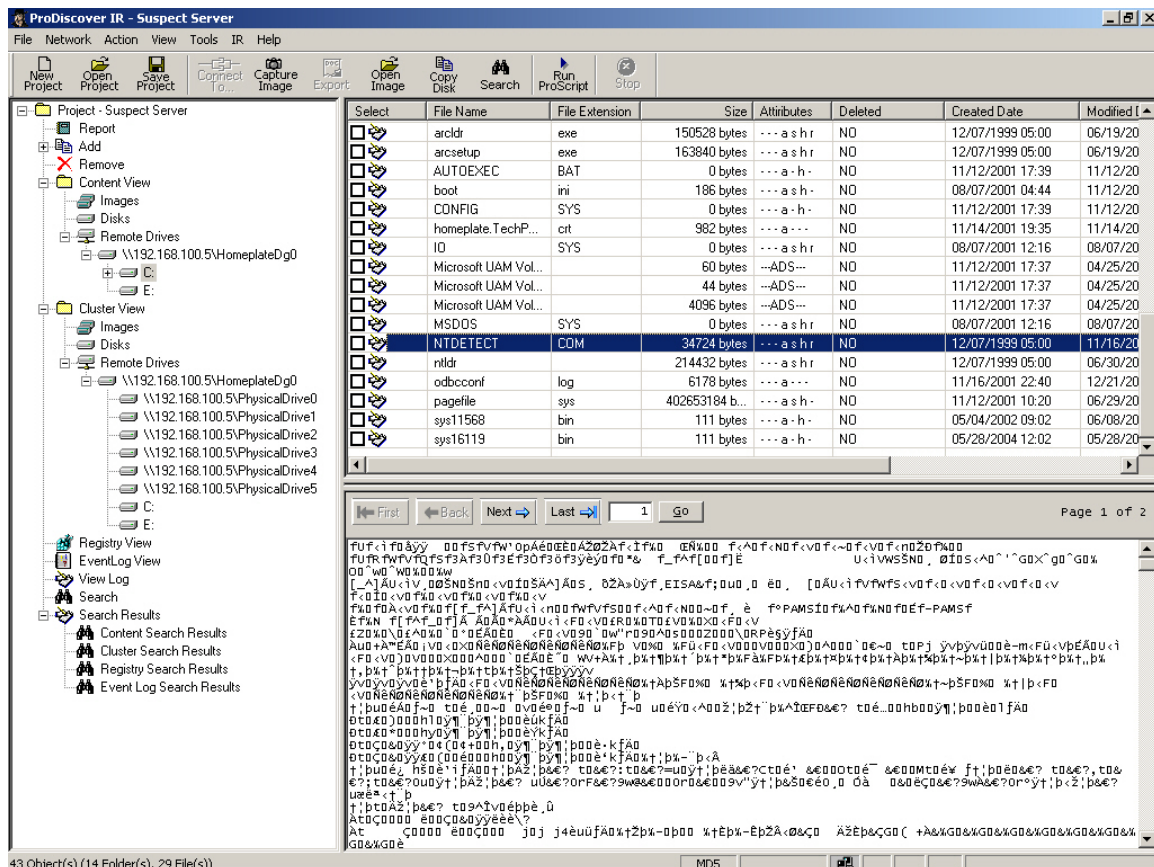
Active Perl Support

- - Commercial support for Active Perl is available through ActiveState at <http://www.ActiveState.com/Support/Enterprise>.
- For peer support resources for ActivePerl issues see: <http://www.ActiveState.com/Support>.

Moving around in ProDiscover

Main Window

ProDiscover's main window is divided into three areas users should become familiar with: left tree-view; upper right work area; and lower right data view area. The separators between all areas are adjustable to allow the user any desired view.



Data View Area Buttons

Note when First, Back, Next, Last and Go buttons appear within the Data View area they allow the user to navigate through pages of large files. (Please see buttons in lower right area.)

On some file systems and images the entire contents of a file or cluster are too large to display in the view area. When this is the case the view area will contain a tag [MORE DATA AVAILABLE] when more data is available. In addition to the tag, the five "navigation" icons will become available in the view area.

First

The **First** icon allows the user to update the view area contents to the first available data segment for the file or cluster selected.

Go

The **Go** icon allows the user to update the view area contents to the data segment number entered for the file or cluster selected.

Last

The **Last** icon allows the user to update the view area contents to the last available data segment for the file or cluster selected.

Next

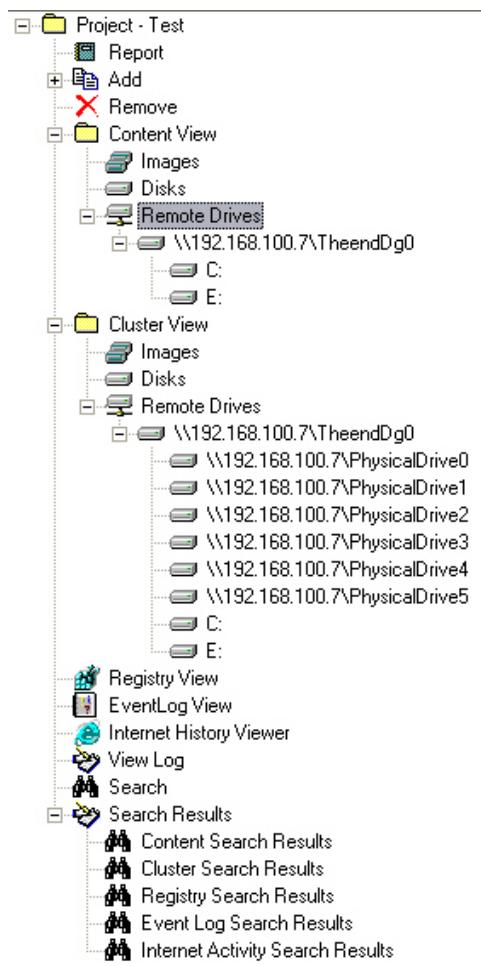
The **Next** icon allows the user to update the view area contents to the next available data segment for the file or cluster selected.

Back

The **Back** icon allows the user to update the view area contents to the previous available data segment for the file or cluster selected.

Tree View Area Items

When a project is opened the user will be presented with a tree-view of selections under the project name as shown below.



Functions available within the tree view are:

- Report
- Add
 - Capture & Add Image
 - Image
 - Disk
- Remove
- Content View
- Cluster View
- Registry View
- EventLog View
- Internet History Viewer
- View Log
- Search
- Search Results
 - Content Search Results
 - Cluster Search Results
 - Registry Search Results
 - EventLog Search Results
 - Internet History Search Results

For a description of each of these commands, please see Appendix A: ProDiscover Menu Commands.

Button Bar

ProDiscover Provides a button bar (sometimes called a Tool Bar) to enable the user to perform commonly used functions quickly.



- New Project
- Open Project
- Save Project
- Connect To...
- Capture Image
- Export
- Open Image
- Copy Disk
- Search
- Stop

For a description of each of these commands, please see Appendix A: ProDiscover Menu Commands.

File Menu

Options available from the File menu enable the user to start a new project, open an existing project, save the current project, save the current project with another name, open an image file, and exit the program.

The File menu, when clicked presents a drop down menu with the following options, which are described in the links below.

- New Project
- Open Project
- Open Image
- Save Project
- Save As
- Preferences
- Print Setup
- Print Report
- Exit

For a description of each of these commands, please see Appendix A: ProDiscover Menu Commands.

Network Menu

The Network Menu contains options supporting ProDiscover's network imaging & analysis functions. Users will use the Network Menu to perform operations such as connect to a remote **PDServer** prior to adding a remote disk.

The Network Menu, when clicked presents a drop down menu with the following options, which are described in the links below.

- Connect To...
- Disconnect
- Encryption
- Release Remote Client

For a description of each of these commands, please see Appendix A: ProDiscover Menu Commands.

Action Menu

Options available from the action menu enable the user to accomplish normal application tasks such as: capture an image, add images and disks to a project, search for keywords, export and clear reports.

The action menu, when clicked presents a drop down menu with the following options:

- Capture Image
- Add
 - Capture & Add Image
 - Image
 - Disk
- Search
- Stop Search

- Clear Report
 - Evidence of Interest
 - Search Results
 - File Signature Mismatch
 - OS Info
 - Clusters of Interest
- Clear Recent Projects List
- Compress
- UnCompress
- Export
- Verify Image Checksum
- Disk Inventory
- OS Info
- Export Evidence of Interest
- Create Report Thumbnails

For a description of each of these commands, please see Appendix A: ProDiscover Menu Commands.

View Menu

The view menu enables the user to view the current project report, the contents of image files and disk as files or clusters and I/O log files. Within the view menu the user can also enable or disable viewing of the ProDiscover startup dialog, tool bar and status bar.

The view menu, when clicked presents a drop down menu with the following options:

- Report
- Content View
- Cluster View
- View Log File
- Startup Dialog
- Tool Bar
- Status Bar

For a description of each of these commands, please see Appendix A: ProDiscover Menu Commands.

Tools Menu

The Tools menu is where the user will find the tools needed for managing disks and images.

The tools menu, when clicked presents a drop down menu with the following options:

- Secure Wipe...
- Copy Disk...
- Copy Selected Files...
- Copy Selected Clusters...
- Filter by Hash Set
- Batch Calculate Hashing...

Signature Matching...
Scan HPA...
Convert Image...
Convert Project Format...
Create remote server disk...

For a description of each of these commands, please see Appendix A: ProDiscover Menu Commands.

IR Menu (ProDiscover IR Edition only)

The IR menu is available only in ProDiscover Incident Response Edition and provides specialized tools for use in incident response and systems auditing.

The IR menu, when clicked presents a drop down menu with the following options:

Find Unseen Processes...
Find Unseen Files...
Create Baseline...
Compare Baseline...
Find Suspect Files...
Get Process List...
Get System State...
Open & Connected IP Ports

For a description of each of these commands, please see Appendix A: ProDiscover Menu Commands.

Help Menu

The Help menu item displays a drop down menu with two options as follows:

- Help Contents: Displays the Help text file describing the various menus, dialog boxes and other controls used in the system in standard Windows help format.
- About ProDiscover: Displays about dialog box containing the product version number, title, copyright etc.

Using ProDiscover

Creating a New Project

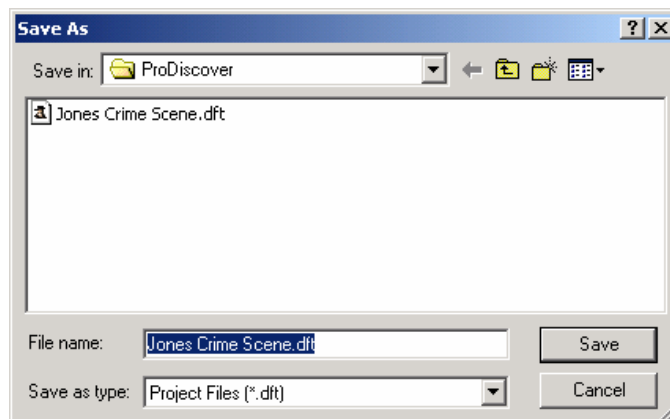
1. Start ProDiscover.
2. ProDiscover presents the launch dialog.



3. Enter a project number, project name, and description of the project in the new project tab option, and then click the **Open** button.
4. ProDiscover will then create a project and generate a template report in the work area.

Save a Project

1. Select save project option from the file menu, or button bar.
2. ProDiscover presents file Save As dialog if the current project has not yet been saved, otherwise the current project file will be updated without further action.



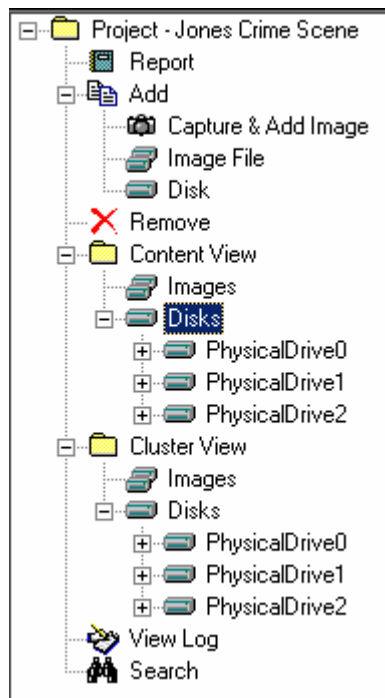
3. Select the destination path and click the **Save** button.
4. ProDiscover saves the project at the path specified.

Preview a directly connected evidence drive

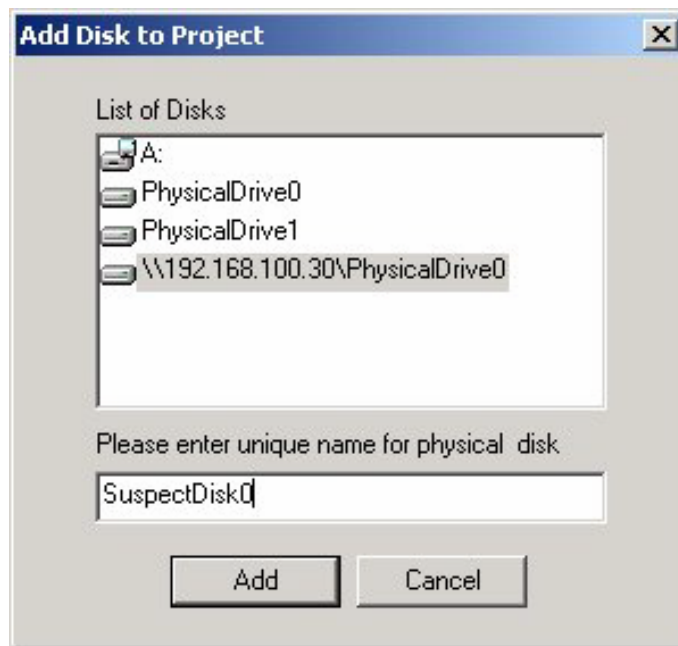
1. Launch ProDiscover.
2. Select **open project** tab option.



3. Select the project file to open and click **Open** button.
4. ProDiscover opens the project file and generates a template report in the work area.
5. Select the **Add Disk** option from the action menu, or tree-view.



6. ProDiscover presents a dialog with all physical disk available for viewing.

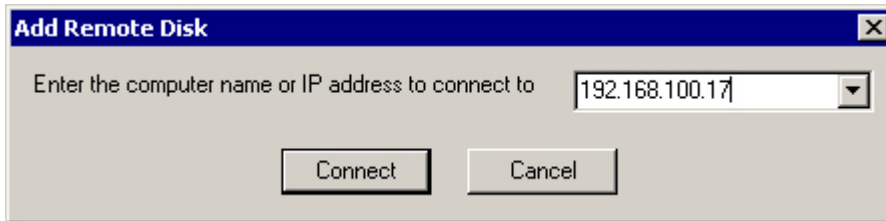


6. ProDiscover then adds the physical disk to the currently active project.
7. Perform actions on the newly added disk such as search, hash compare and recovery).

Conducting Live Preview of a Remote Disk

Prior to previewing a remote disk users will need to create a **PDServer** disk and run PDserver on the remote system.

1. Once **PDServer** is running on the remote system, from within an active project in ProDiscover use the "Network" menu to select "Connect To..." and the following dialog box will appear.



2. If the user is connecting to a **PDServer** running in Stealth Mode with a password set the ProDiscover client will display a dialog box asking for the password prior to connection. Even if encryption mode is not set for encryption is used to create a secure channel for all communications setup to prevent password sniffing and man-in-the middle attacks.



3. Once the connection is established users follow standard procedures for previewing a directly connected disk. Previewing speed can vary greatly and is dependant on many factors such as network topology and performance. When encryption mode is set the added overhead can reduce preview performance by up to a factor of two.

Capture an image of an attached drive

1. Ensure the desired evidence drive is attached to the ProDiscover system.
2. Select the capture image option from the action menu item, or button bar.
3. ProDiscover presents the capture image dialog.

Capture Image

Source Drive: F:\ [ImageDrive]

Destination: F:\SuspectImage.eve >> Split

Image Format: ProDiscover Format (recommended)

Total sectors to capture : 156296384 HPA

ProDiscover Image

Technician Name: Chris B

Image Number: 039432E

Description :
Suspect Suspect Boot Drive

Compression
☐ Yes
☒ No

Password...

OK Cancel

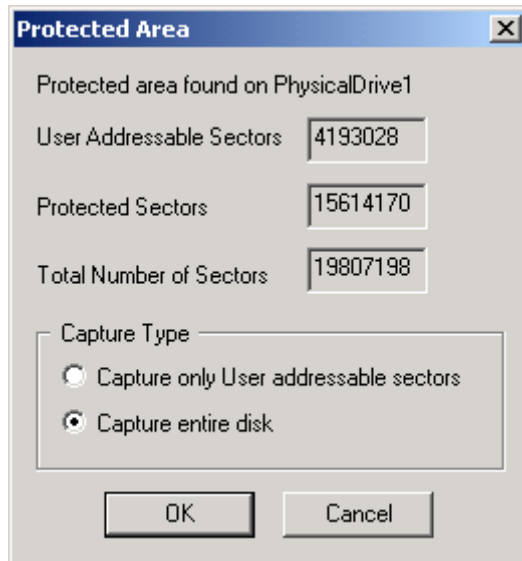
4. Select the drive to be captured, destination path for the image file to be saved into, compression and password protection of the image file and specify the technician name, image number, description of the image file.

Note: When imaging dynamic disk containing disk groups such as RAID (Redundant Array of Independent Disks) sets, individual disks belonging to the disk group will be captured to different files as physical disks. At the end of the capture, a .PDG (ProDiscover Disk Group) file will be created. The .PDG file contains the information about the image files in the group along with the disk's identifiers for cross-referencing.

5. Users also have the option to select the desired image format. ProDiscover recommends using the ProDiscover format which includes adding metadata to the image containing information for password protection, time zone, investigator and compression. A technical description of the ProDiscover image format can be found on the Technology Pathways web site in the resources section. Alternately, users can select to create an image in the UNIX style 'dd' format which creates a flat bit-stream image and a corresponding hash file using the selected hashing algorithm.

the corresponding hash file will be placed in the image directory and named the same as the image using a .md5 or .sha file extension.

6. If ProDiscover detects the image has a Hardware Protected Area the **"HPA"** button will be enabled. Selecting the button will display the following dialog allowing user control over the sectors to be imaged.

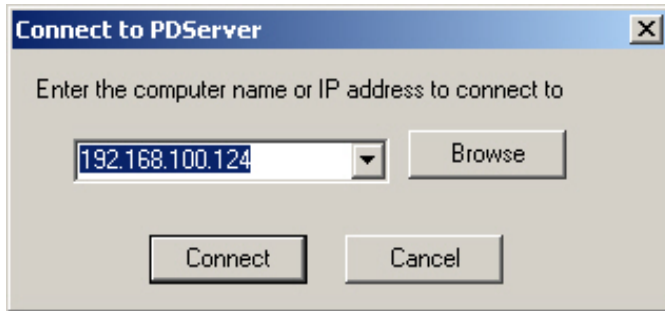


7. To compress the image select "Yes" to compression and ProDiscover will compress the image and save it as *.cmp. Note that compressing an image requires more time to capture due to the compression overhead.
8. Click "OK".
9. ProDiscover reads the drive connected bit-by-bit and creates an image file in the specified location. The image file will contain an exact replica of the original disk, plus a few bites of checksum and log data.
10. ProDiscover will create a log file if there are any I/O errors.

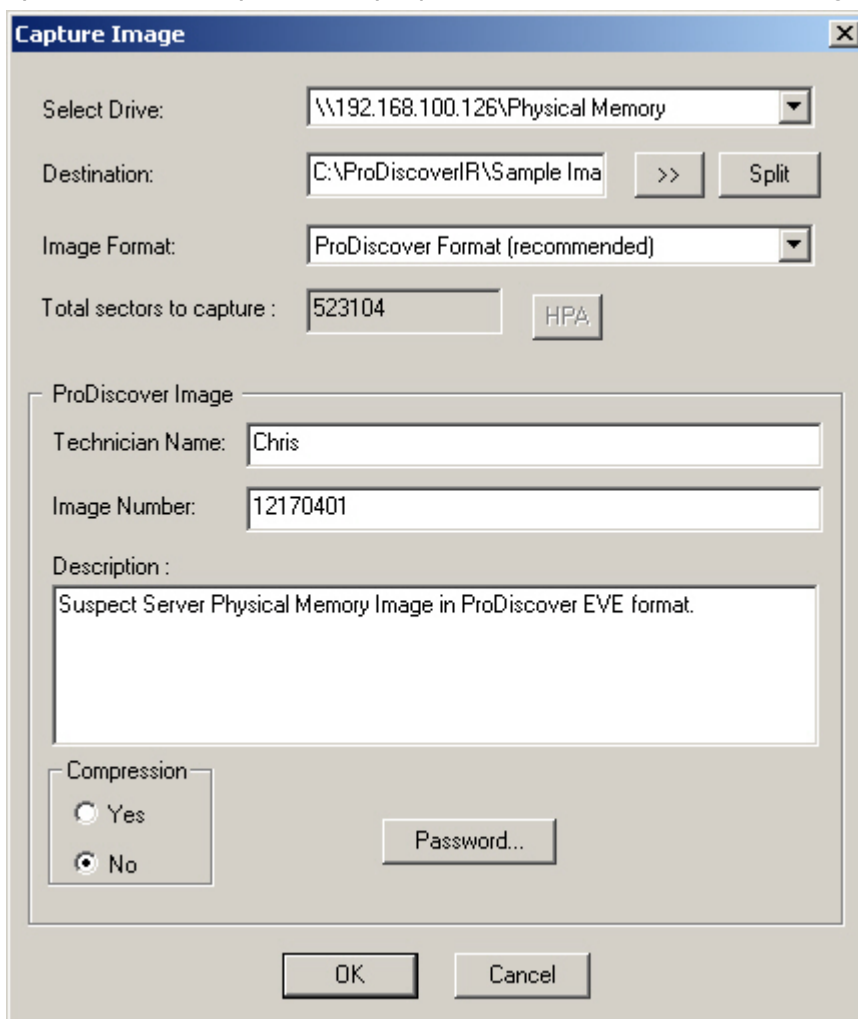
Capturing Physical Memory

When connecting to remote systems using ProDiscover Incident Response or Investigator users may find it useful to capture the live volatile physical memory of the suspect system. Collection of physical memory images allows the investigator to conduct searches of the physical memory image to find indications of compromise or passwords cached in memory. Passwords cached in memory may be useful to investigators later in the analysis of encrypted documents.

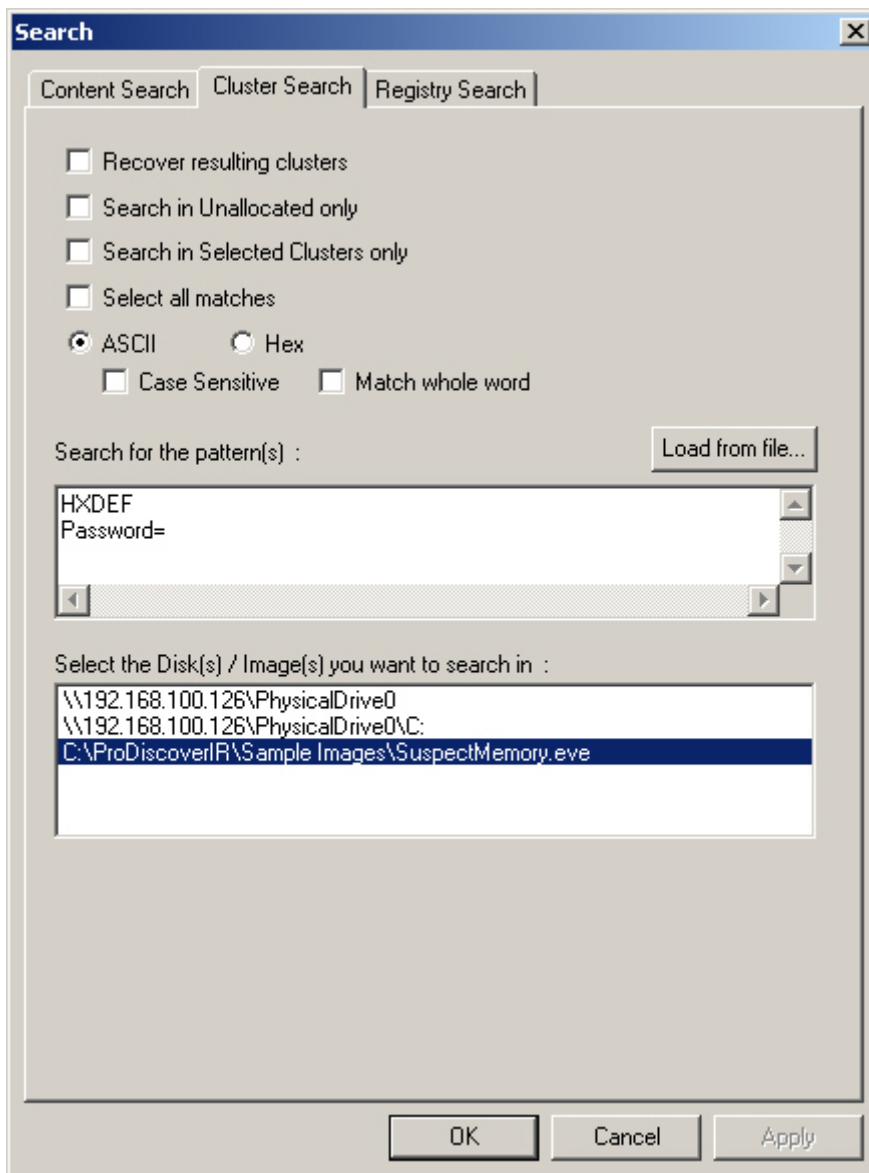
To create an image of a remote systems physical memory users should first ensure the PDServer remote agent is running on the remote system then connect to the remote system using the "Connect To..." button bar icon or network menu item.



Once connected to the remote system users can image the remote systems physical memory by choosing the "Capture Image" button bar icon or Action menu item. In the dialog box that appears users should follow the normal steps for capturing an image and select the remote systems "SystemNameOrIP\PhysicalMemory" option under "Select Drive" in the dialog as seen below.



The physical memory image can be created in the ProDiscover EVE format or UNIX dd style format just as with disk images. Once the image is created it can be added to the current project using "add image" and searched with the "Search | Cluster Search" function as seen below. There is no content-view available for raw physical memory images.



ProDiscover IR - SuspectServer

File Network Action View Tools IR Help

New Project Open Project Save Project Connect To Capture Image Export Open Image Copy Disk Search Stop

Project - SuspectServer

- Report
- Add
- Remove
- Content View
 - Images
 - Disks
 - Remote Drives
- Cluster View
 - Images
 - C:\ProDiscover\IR\Sample Images\S...
 - Disks
 - Remote Drives
- Registry View
 - \\192.168.100.126\PhysicalDrive0\C:\V...
 - View Log
- Search
 - Search Results
 - Content Search Results
 - Cluster Search Results
 - Registry Search Results

Search 1

Search terms: All Patterns Add to Report Patterns Selection Filter

Select	Cluster Number	Found in
☐	31F43 (204611)	C:\ProDiscover\IR\Sample Images\SuspectMem...
☐	31F49 (204617)	C:\ProDiscover\IR\Sample Images\SuspectMem...
☐	31F68 (204651)	C:\ProDiscover\IR\Sample Images\SuspectMem...
☐	31F6F (204655)	C:\ProDiscover\IR\Sample Images\SuspectMem...
☒	32160 (205152)	C:\ProDiscover\IR\Sample Images\SuspectMem...
☐	322A8 (205480)	C:\ProDiscover\IR\Sample Images\SuspectMem...
☐	3240B (205835)	C:\ProDiscover\IR\Sample Images\SuspectMem...
☐	3240C (205836)	C:\ProDiscover\IR\Sample Images\SuspectMem...
☐	326ED (206573)	C:\ProDiscover\IR\Sample Images\SuspectMem...
☐	32749 (206665)	C:\ProDiscover\IR\Sample Images\SuspectMem...
☐	32B70 (207728)	C:\ProDiscover\IR\Sample Images\SuspectMem...
☐	32C77 (207991)	C:\ProDiscover\IR\Sample Images\SuspectMem...
☐	32CCD (208077)	C:\ProDiscover\IR\Sample Images\SuspectMem...
☐	3301D (208925)	C:\ProDiscover\IR\Sample Images\SuspectMem...
☐	3301D (208925)	C:\ProDiscover\IR\Sample Images\SuspectMem...

```

00000000 5B 48 69 64 64 65 6E 20 54 61 62 6C 65 5D 00 0A [Hidden Table]..
00000010 68 78 64 65 66 2A 0D 0A 72 63 6D 64 2E 65 78 65 hxdmf*..rcmd.exe
00000020 00 0A 00 0A 58 52 6F 6F 74 20 50 72 6F 63 65 73 ...[Root Proces
00000030 73 65 73 5D 00 0A 68 78 64 65 66 2A 0D 0A 72 63 ses]..hxdmf*..rc
00000040 6D 64 2E 65 78 65 0D 0A 00 0A 5B 48 69 64 64 65 md.exe....[Hidde
00000050 6E 20 53 65 72 76 69 63 65 73 5D 0D 0A 48 61 63 n Services]..Hac
00000060 68 65 72 44 65 66 65 6E 64 65 72 2A 0D 0A 0D 0A kerDefender*...
00000070 5B 48 69 64 64 65 6E 20 52 65 67 4B 65 79 73 5D [Hidden RegKeys]

00000080 0D 0A 48 61 63 6B 65 72 44 65 66 65 6E 64 65 72 ..HackerDefender
00000090 30 37 33 0D 0A 4C 45 47 41 43 59 5F 48 41 43 4B 073..LEGACY_HACK
000000A0 45 52 44 45 46 45 4E 44 45 52 30 37 33 0D 0A 0D ERDEFENDER073...
000000B0 0A 5B 48 69 64 64 65 6E 20 52 65 67 56 61 6C 75 .[Hidden RegValu
000000C0 65 73 5D 0D 0A 0D 0A 5B 53 74 61 72 74 75 70 2D es]....[Startup
000000D0 52 75 6E 5D 0D 0A 0D 0A 5B 53 65 74 74 69 6E 67 Run]....[Setting
000000E0 73 5D 0D 0A 50 61 73 73 77 6F 72 64 3D 6F 77 6E s]..Password=own
000000F0 65 64 0D 0A 42 61 63 6B 64 6F 6F 72 53 68 65 6C ed..BackdoorShel

00000100 6C 3D 68 78 64 65 66 DF 24 2E 65 78 65 0D 0A 53 1=hxdmf$.exe..s
00000110 65 72 76 69 63 65 4E 61 6D 65 3D 48 61 63 6B 65 erviceName=Hacke
00000120 72 44 65 66 65 6E 64 65 72 30 37 33 0D 0A 44 69 rDefender073..Di
00000130 73 70 6C 61 79 4E 61 6D 65 3D 48 58 44 20 53 65 splayName=HxD Se
00000140 72 76 69 63 65 20 30 37 33 0D 0A 53 65 72 76 69 rvicse 073..Servi
00000150 63 65 44 65 73 63 72 69 70 74 69 6F 6E 3D 70 6F cedescription=po
00000160 77 65 72 66 75 6C 20 4E 54 20 72 6F 6F 74 68 69 werful NT rootki
00000170 74 0D 0A 0D 0A 5B 43 6F 6D 6D 65 6E 74 73 5D 0D t....[Comments].

00000180 0A 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000190 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....

```

4 occurrences found.

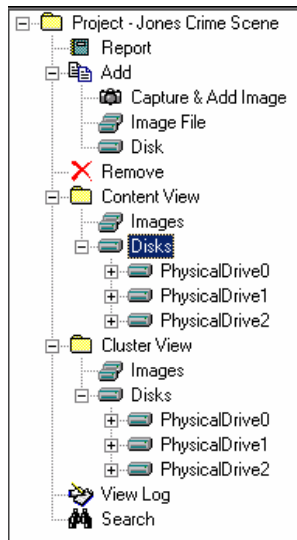
MDS

Add an image file to a project

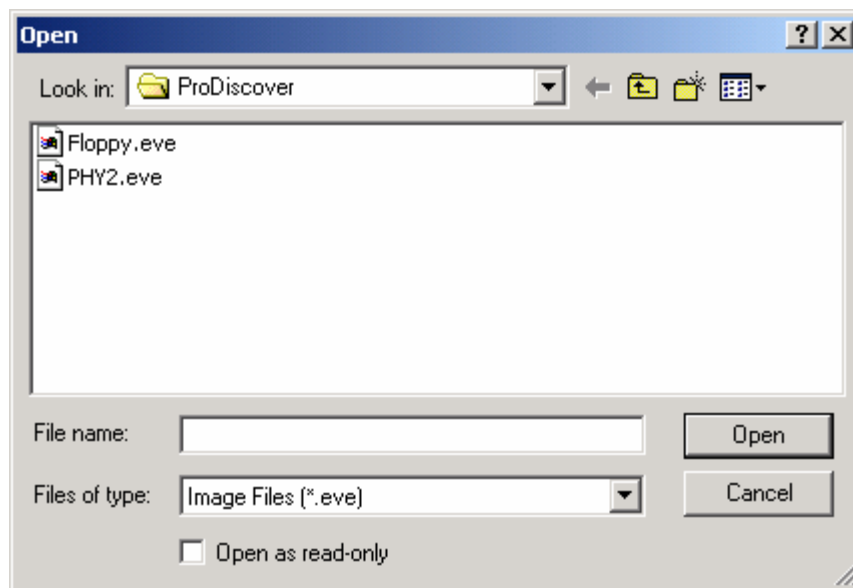
1. Launch ProDiscover.
2. Select **open project** tab option.



3. Select the project file to open and click **Open** button.
4. ProDiscover opens the project file and generates a template report in the work area.
5. Select the **Add Image** option from the action menu, or tree-view. Users may also right-click on "Disks", "Images" or "Remote Drives" from Content-view to add a disk, image or remote drive to the project.



6. ProDiscover presents the file open dialog.



7. Select the desired image file and Click **Open** button. If the image is of a Windows NTFS Dynamic Disk, users should select the image's corresponding *.pdg file which describes the disk group. If the image was a ProDiscover Split image, users should select the *.pds file which describes all split files comprise the total disk image.
8. UNIX style "dd" images can be added to projects provided with or without the .eve file extension. To add a dd image to the project without an expected extension choose "All Files (*.*)" from the "File of Types" Drop down list. If the "dd" image is split into several images they should be numbered sequentially and all contain a .eve file extension. Once the image files are named and numbered correctly a corresponding *.pds file should be created in the following format:

DD-SplitImage

D:\Images\Splits\dd\Split0.eve

D:\Images\Splits\dd\Split1.eve

D:\Images\Splits\dd\Split2.eve

D:\Images\Splits\dd\Split3.eve

D:\Images\Splits\dd\Split4.eve

9. Note that all split image file should be split in sizes which are multiples of 512. To add the split "dd" image users should select the split.pds file created above.
10. ProDiscover then adds the image file to the currently active project.

Add a UNIX "dd" image file to a project

ProDiscover supports analysis of "dd" images on supported file systems for forensics examiners using UNIX "dd", or the Win32 "dd" port to create physical or logical images.

UNIX style "dd" images can be added to projects. If the "dd" image is split into several images they should be numbered sequentially and all contain a .eve or any other desired file extension. Once the image files are named and numbered correctly a corresponding *.pds file should be created in the following format:

DD-SplitImage
Split0.eve
Split1.eve
Split2.eve
Split3.eve
Split4.eve

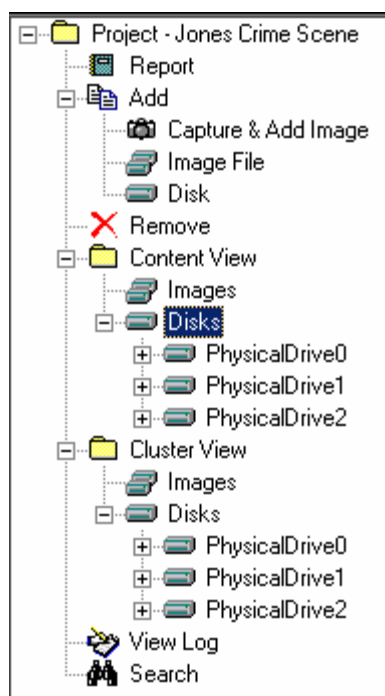
Note that all split image file should be split in sizes which are multiples of 512. To add the split "dd" image users should select the split.pds file created above.

To add a UNIX "dd" image:

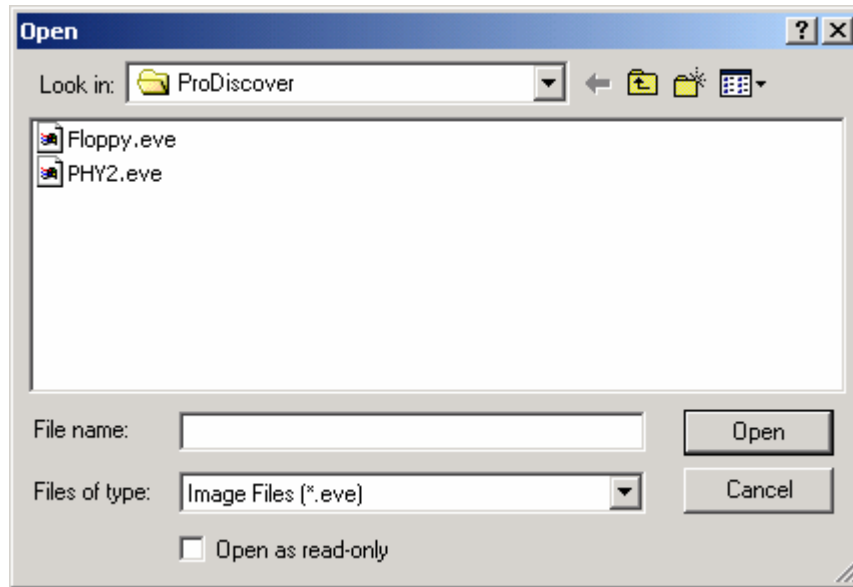
1. Ensure your "dd" image has the file extension ".eve".
2. Launch ProDiscover.
3. Select **open project** tab option.



3. Select the project file to open and click **Open** button.
4. ProDiscover opens the project file and generates a template report in the work area.
5. Select the **Add Image** option from the action menu, or tree-view. Users may also right-click on "Disks", "Images" or "Remote Drives" from Content-view to add a disk, image or remote drive to the project.



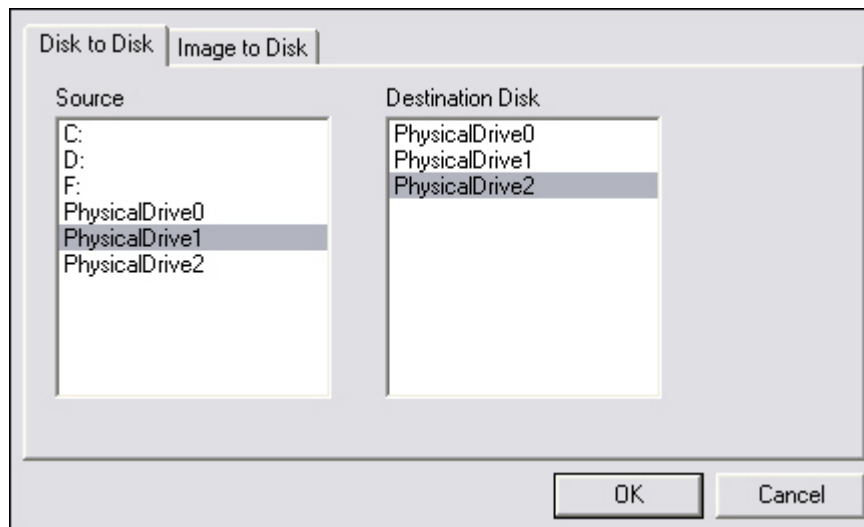
6. ProDiscover presents the file open dialog.



7. Select the desired image file and Click **Open** button.
8. ProDiscover then adds the image file to the currently active project.

Copy a directly connected drive to another directly connected drive

1. Ensure the desired evidence drive is attached to the installed ProDiscover system.
2. Select the copy disk option from the action menu, or button bar.

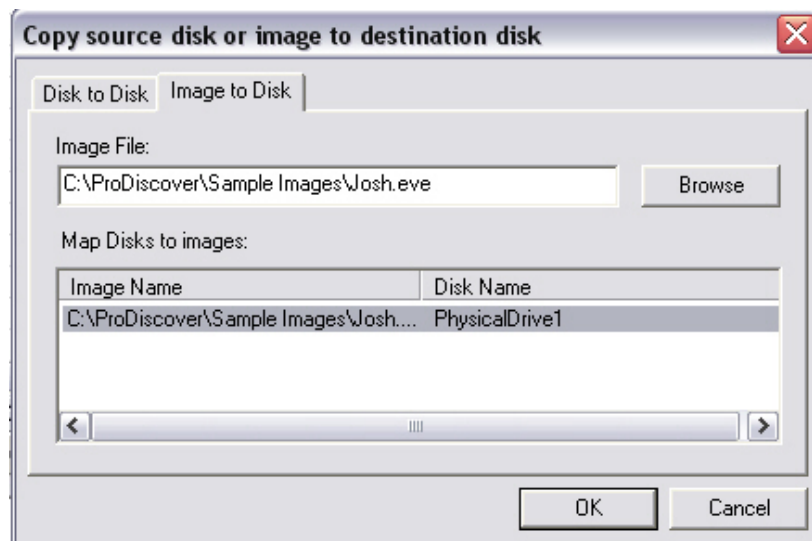


3. ProDiscover presents a dialog with the list of all local drives on the system. **Note: only physical disk large enough to accommodate the selected source disk will be shown in the destination disk section.**

4. Select the source and destination disk, then click **OK**.
5. ProDiscover copies the source disk to the destination disk.

Restore an Image to directly connected drive

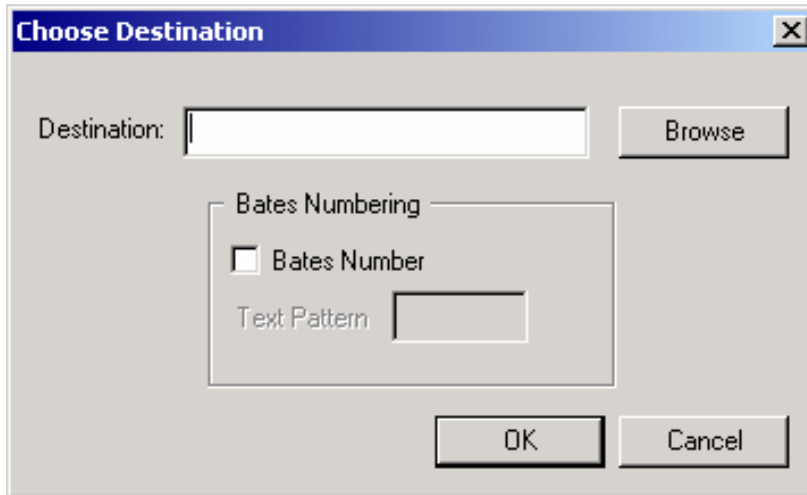
1. Ensure the desired destination drive is attached to the installed ProDiscover system and its size will accommodate the original image.
2. Select the copy disk option from the tools menu, or button bar.



3. ProDiscover presents a dialog with the list of all local drives on the system.
4. Select **"Image"** from the source section of the dialog box.
5. Select the **"Browse"** button and locate the desired image. **Note: Native ProDiscover images and UNIX "dd" images can be restored.**
6. Select the desired destination disk, and then click **OK**.
7. ProDiscover restores the image to the destination disk.

Copy Selected Files

In many cases you will want to recover items to another location in preparation for evidence presentation or further analysis. The "Copy Selected Files" option from the Tools Menu provides users with the ability to conduct a batch recovery/transfer of all items marked as "Evidence of Interest" by enabling the "Selected" Tag within "Content View".



List detail information about image files associated with a project

1. Select "**Content View | Images**", or "**Cluster View | Images**" from the tree-view.
2. ProDiscover lists detailed information of all image files associated with a project.

View the contents of a directly connected disk as files

1. Ensure the desired evidence disk is connected to the ProDiscover system and the desired disk has been added to the current project.
2. Select the "**Content View | Disks | Physical Drive | Partition**" option from the Menu or tree-view. Note: Disk containing a Hardware Protected Area will display [HPA] after a partition to indicate any file systems detected within the HPA. See [Advanced tips and tricks](#) for more information on the HPA.
3. Select the desired disk partition.
4. ProDiscover displays the contents of the disk.
5. Select a file or directory to view from the work area.
6. ProDiscover displays the contents of that file at the bottom of the main window.
7. Double click on a file.
8. ProDiscover displays the contents of the file in the default file viewer. If no viewer has been set, ProDiscover will launch an "**Open With**" dialog box asking the user to select an application to open the file.

View the contents of a disk, or image file as clusters

1. Select "**Cluster View | Disks, or Image | Physical Drive | Partition**" from the View Menu or tree-view. Disk containing a Hardware Protected Area will display [HPA] after a partition to indicate any file systems detected within the HPA. See [Advanced tips and tricks](#) for more information on the HPA.
2. ProDiscover presents a graphic representation of clusters for image file, or disk in the work area.
3. Select an individual cluster.
4. ProDiscover displays the contents of that cluster at the bottom of the main window.

Viewing the Windows Event Logs

ProDiscover allows users to add the Windows Event Logs to a project from images or directly connected disks. Once the event logs are added to a current project, users can review individual log entries and select as evidence of interest if needed.

The following steps allow users to add a Windows Event Log to the current project:

Add an image file or disk to the current project.

Navigate to the Windows installation directory (C:\Windows, C:\Winnt, etc.) on any partition from content view.

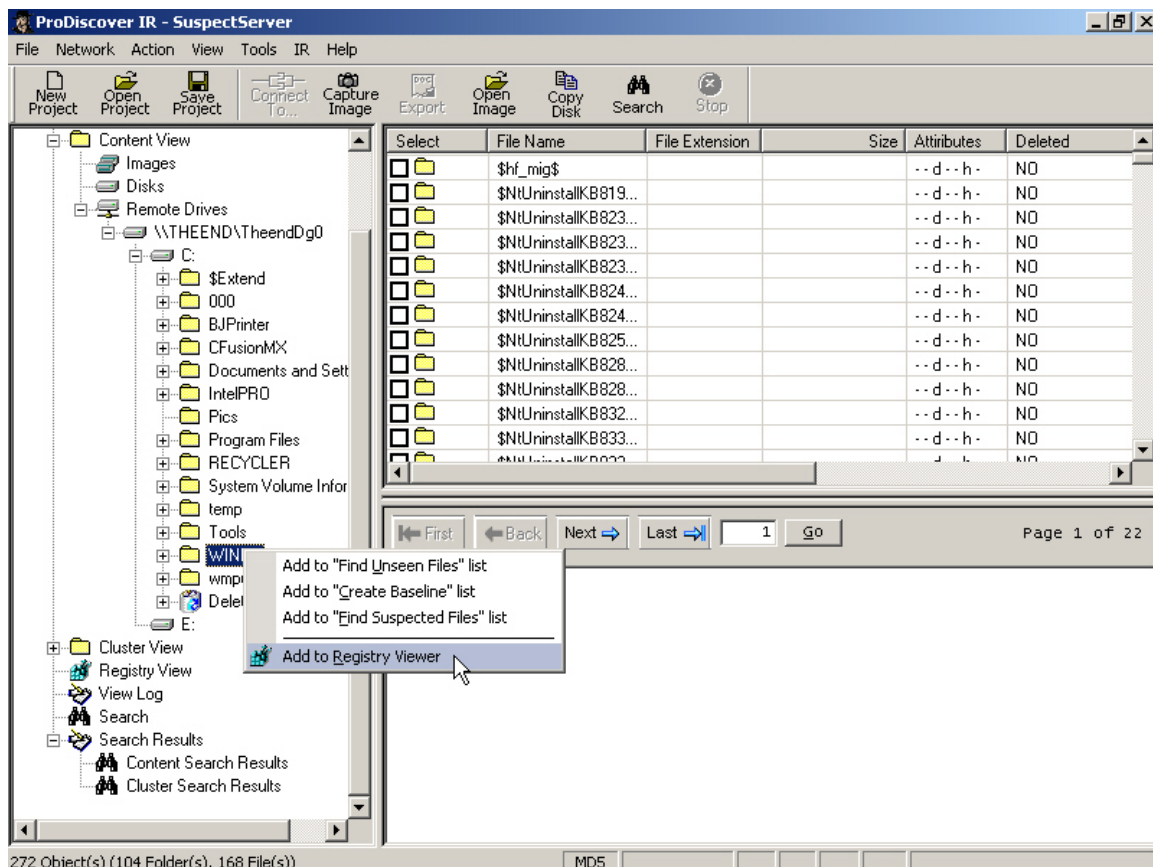
Highlighting the Windows installation directory from content view, right-click on the directory and choose "Add to Event Log Viewer".

The Windows event logs from the selected installation will be available for view from the "Event Log View" tree-view item.

View Windows Registry

The registry viewer allows investigators to browse the registry of a Windows system and select individual registry keys as evidence of interest. To process the windows registry ProDiscover needs to read several files on the disk in addition to individual registry files themselves.

To process registry files from the local or remote disk or image users should highlight the windows system directory in content view, right-click and choose "Add to Registry Viewer". The default system directory on a Windows NT 4.0 system is Winnt. In Windows XP the default system directory is Windows. Once the user selects "Add to Registry Viewer" as seen below.



ProDiscover will scan the directory structure and extract the files needed to process the registry view allowing the registry to be viewed as seen below.

The screenshot shows the ProDiscover IR - SuspectServer application. The 'Registry View' pane on the left displays the following tree structure:

- \\THEEND\\PhysicalDrive0\\C:\\WINNT
 - HKEY_CLASSES_ROOT
 - HKEY_LOCAL_MACHINE
 - SAM
 - SECURITY
 - SOFTWARE
 - SYSTEM
 - ControlSet001
 - Control
 - Enum
 - Hardware Profiles
 - Services
 - .NET CLR Data
 - Performance (selected)
 - .NET CLR Networking
 - .NETFramework
 - {2B5B1EB3-D583-494F-AAD0-03}
 - Abiosdsk
 - abp480n5
 - ACPI
 - ACPIEC
 - adpu160m
 - AFD
 - agp440
 - Aha154x
 - aic116x
 - aic78u2
 - aic78xx
 - Alerter

The right pane displays a table of registry values:

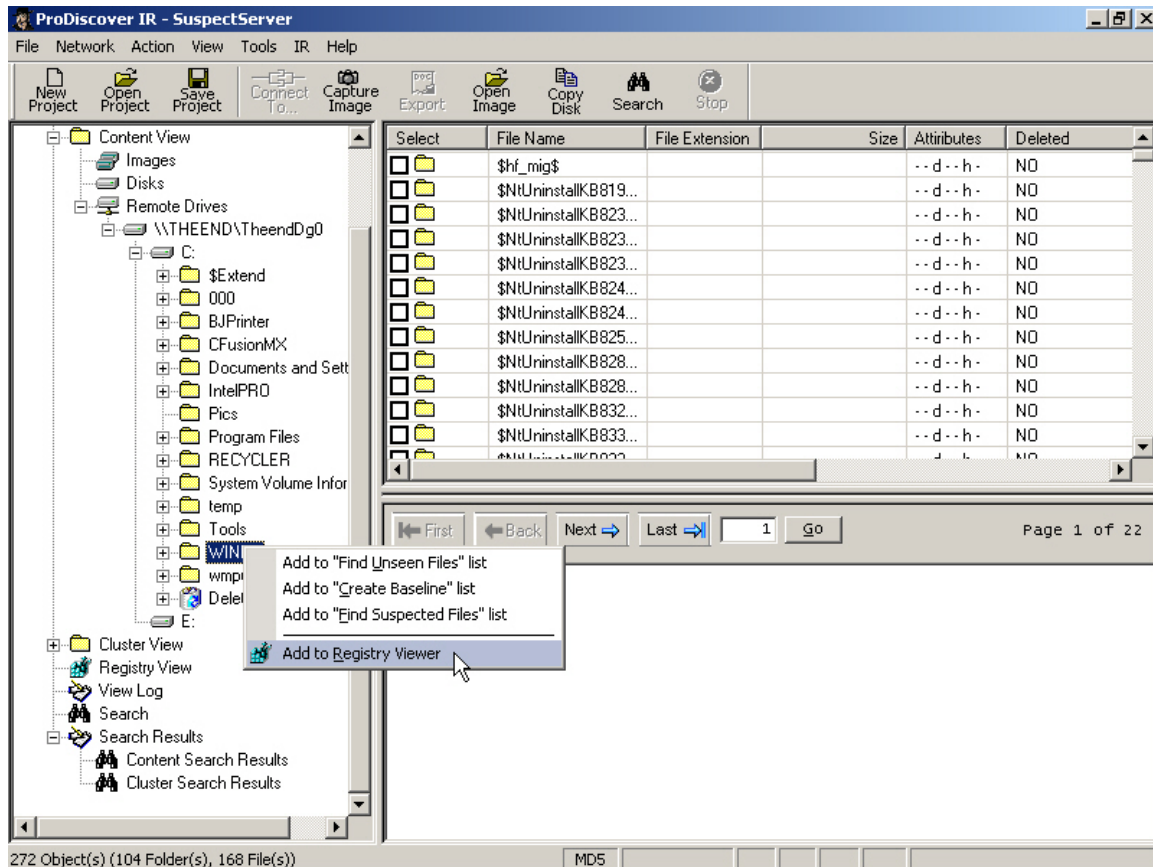
Select	Name	Type	Data
☐	(Default)	REG_SZ	(value not set)
☐	Open	REG_SZ	OpenPerformanceData
☐	Collect	REG_SZ	CollectPerformanceData
☐	Close	REG_SZ	ClosePerformanceData
☐	Library	REG_SZ	netfxperf.dll
☐	Counter Types	REG_BIN	36 00 35 00 35 00 33 00 36 00 0...
☐	Counter Names	REG_BIN	53 00 71 00 6C 00 43 00 6C 00 6...
☐	Last Counter	REG_DWORD	0x00000c92 (3218)
☐	Last Help	REG_DWORD	0x00000c93 (3219)
☐	First Counter	REG_DWORD	0x00000c86 (3206)
☐	First Help	REG_DWORD	0x00000c87 (3207)
☐	Object List	REG_SZ	3206
☐	WbemAdapFileTime	REG_BIN	00 AD 3D 41 4F D9 C2 01
☐	WbemAdapFileSize	REG_DWORD	0x00008000 (32768)
☐	WbemAdapStatus	REG_DWORD	0xffffffff (-1)

The status bar at the bottom shows the path: HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\NET CLR Data\Perfor MD5

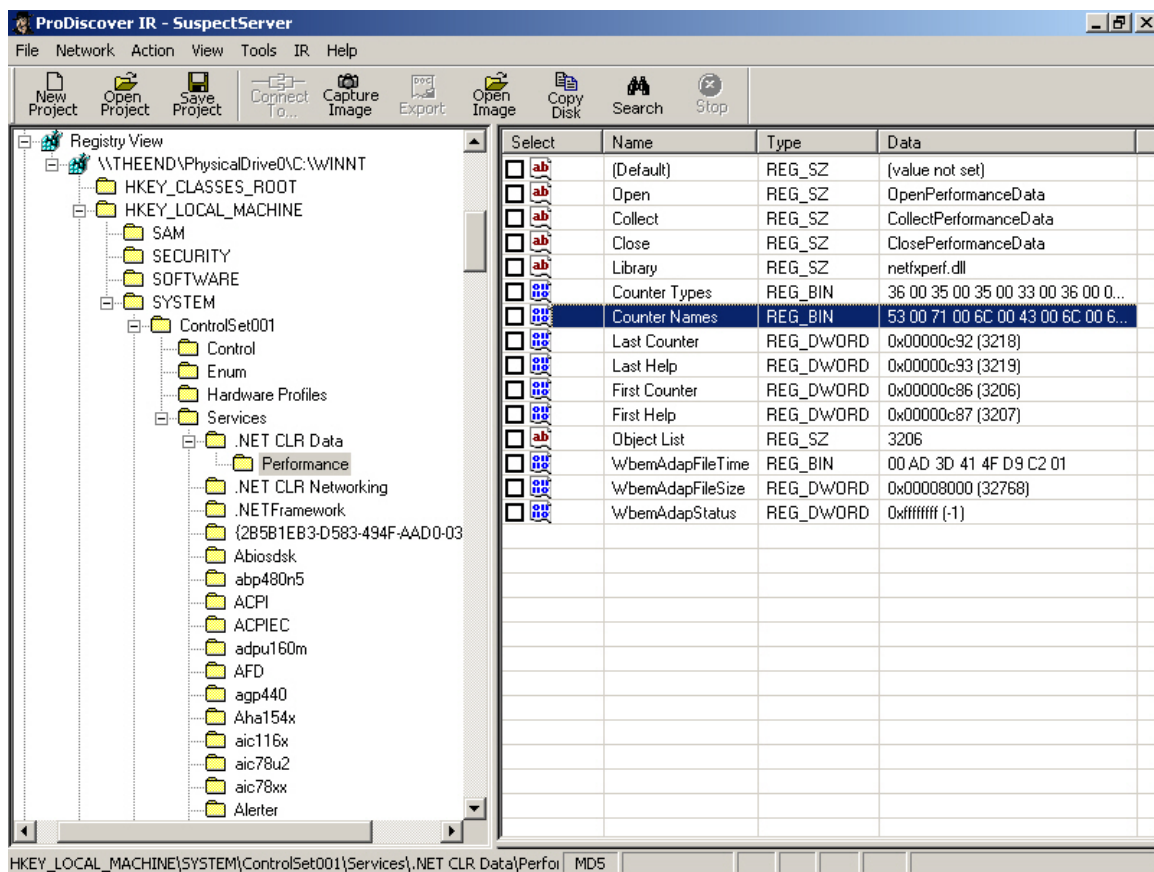
Search the Windows Registry

Prior to searching a Windows Registry, users must first add the registry to their project using the following procedures.

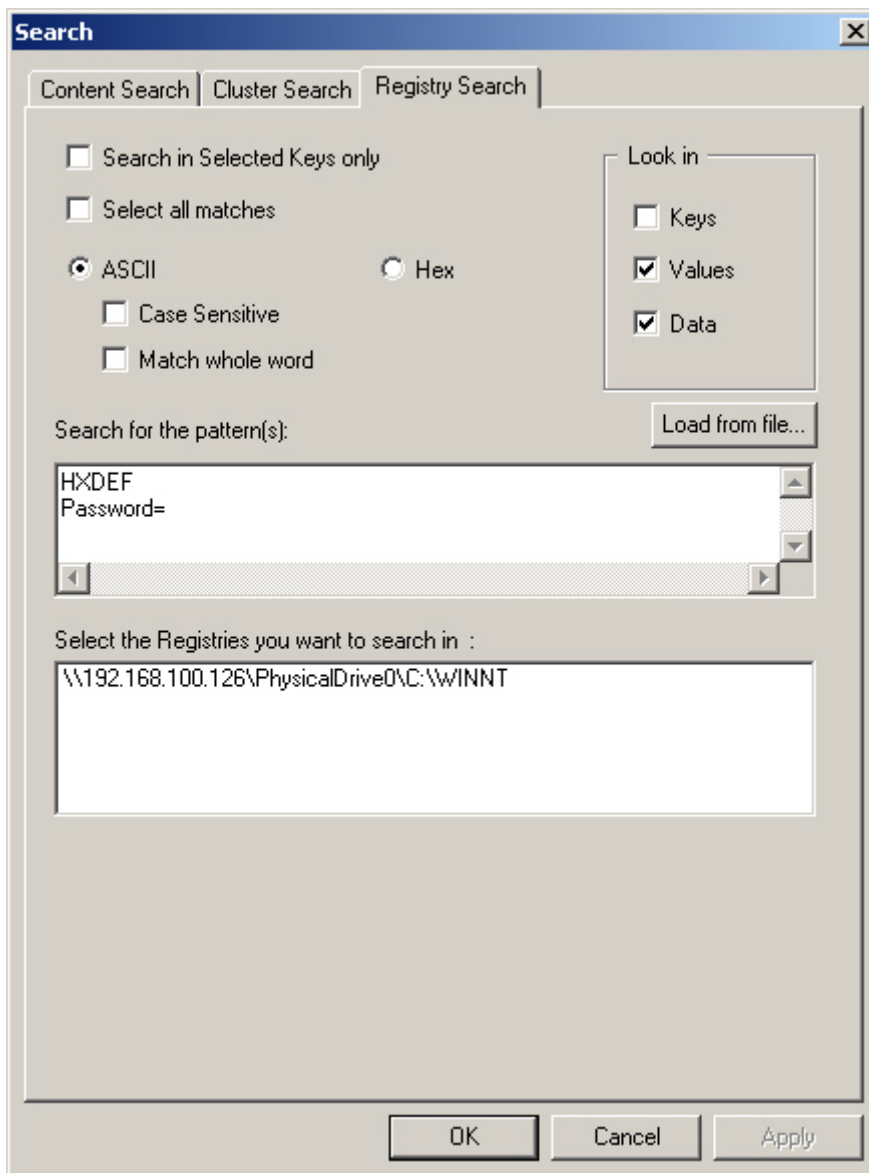
To process registry files from the local or remote disk or image users should highlight the windows system directory in content view, right-click and choose "Add to Registry Viewer". The default system directory on a Windows NT 4.0 system is Winnt. In Windows XP the default system directory is Windows. Once the user selects "Add to Registry Viewer" as seen below.



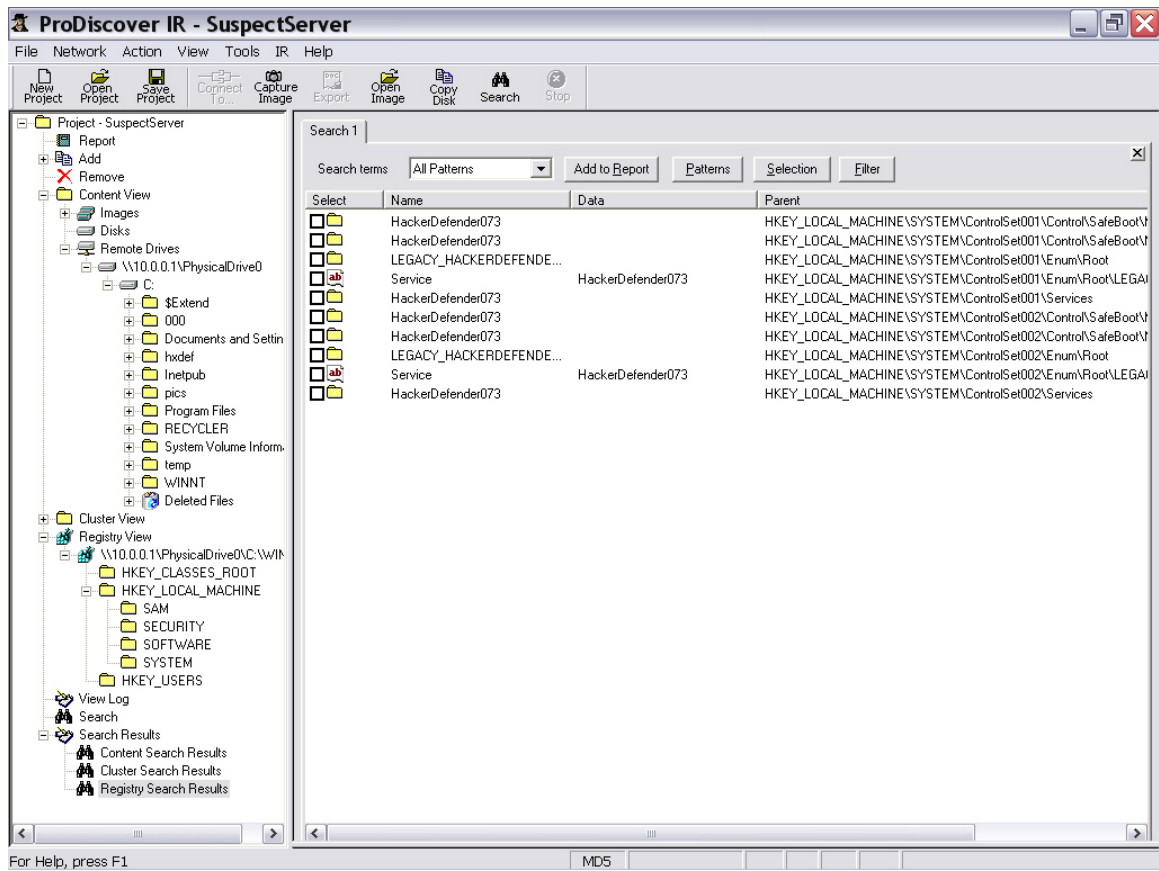
ProDiscover will scan the directory structure and extract the files needed to process the registry view allowing the registry to be viewed as seen below.



Once the desired registry has been added to the current project, users can search the registry for keywords using the "Search" option from the ProDiscover button bar.

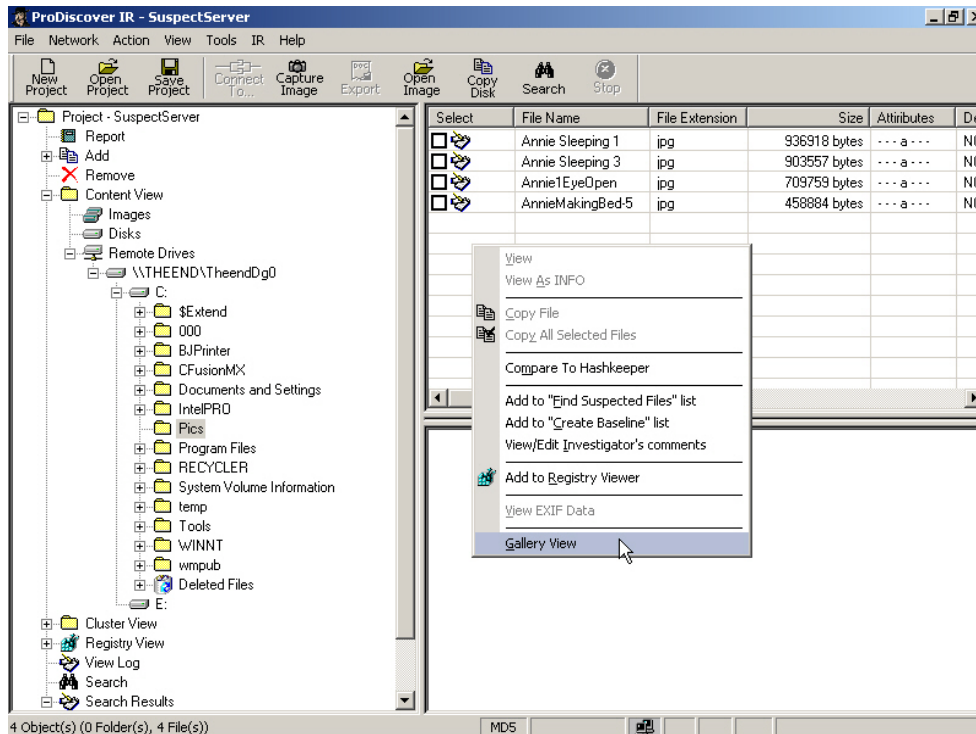


Search results will be displayed as seen below in the "Registry Search Results" tree-view item.

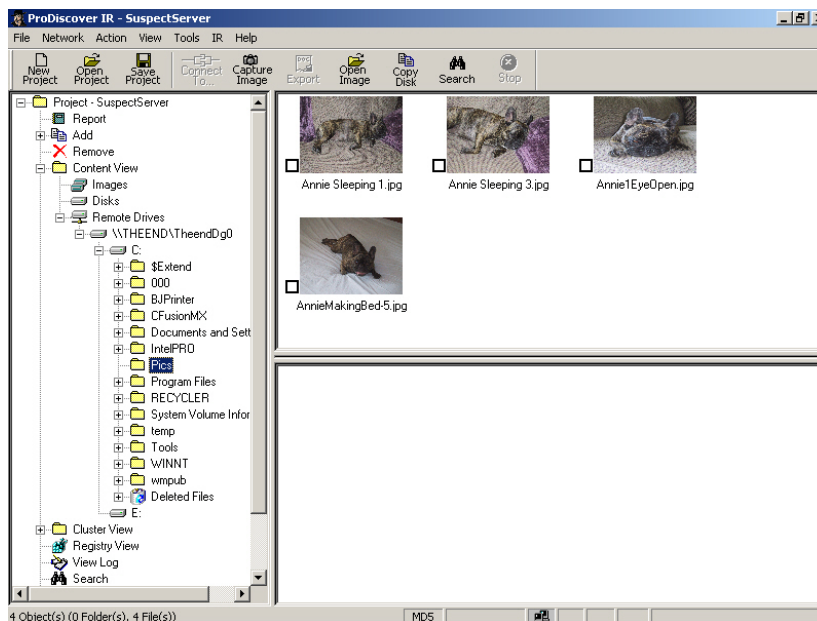


View Graphic Files in Gallery View

In situations where users need to view the contents of a large number of graphic files in a given directory ProDiscover offers a "Gallery View" function. To shift into a gallery view mode users need only choose the "Gallery View" menu option from the "View" menu or right click over the work area as seen below.



Once the user selects "Gallery View" the work area view will display a thumbnail of all images within the selected directory as seen below.



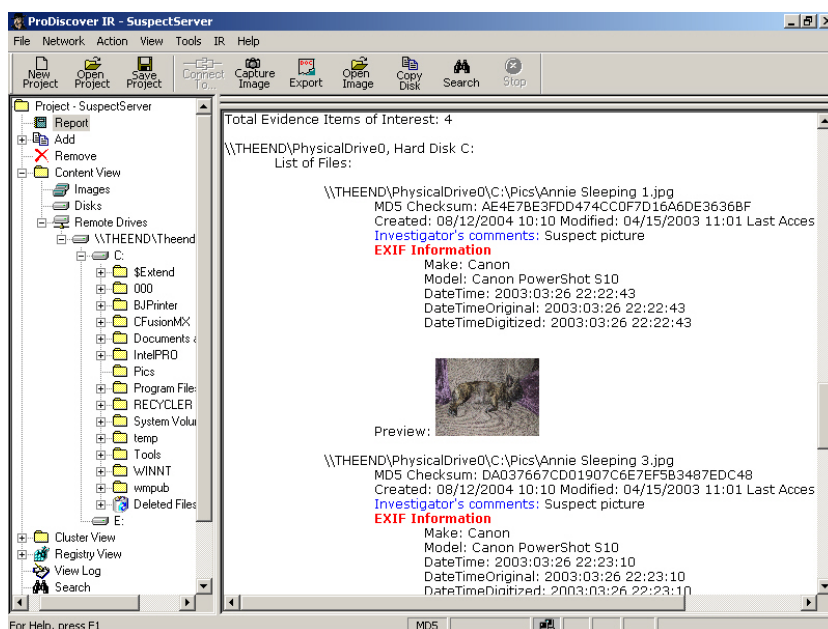
Adding Thumbnail Images to Report for Graphic Evidence

Users may desire to add preview thumbnail images along with information provided to the standard project report. To add graphic thumbnail preview images users should use the "Appearance" tab of the "Preferences" File menu option. In the appearance section users will find the following two options:

"Add thumbnail image to report for graphic files" (default unchecked) when checked will cause a thumbnail image to be created and added to the report for any graphic file which is selected as evidence of interest. For users who choose this option after graphic files have been added as evidence of interest they can use the Action menu's "Create report thumbnails" option to add thumbnails to the report.

"Create thumbnails on load" (default unchecked) when checked causes ProDiscover to automatically add thumbnail images to the report when opened. **Warning: a large report, with many graphic files selected as evidence of interest, can cause a significant delay while loading a project file.**

After choosing the desired settings thumbnail images will be added to the live ProDiscover project report (as seen below) as well as any report that is exported in the RTF format.

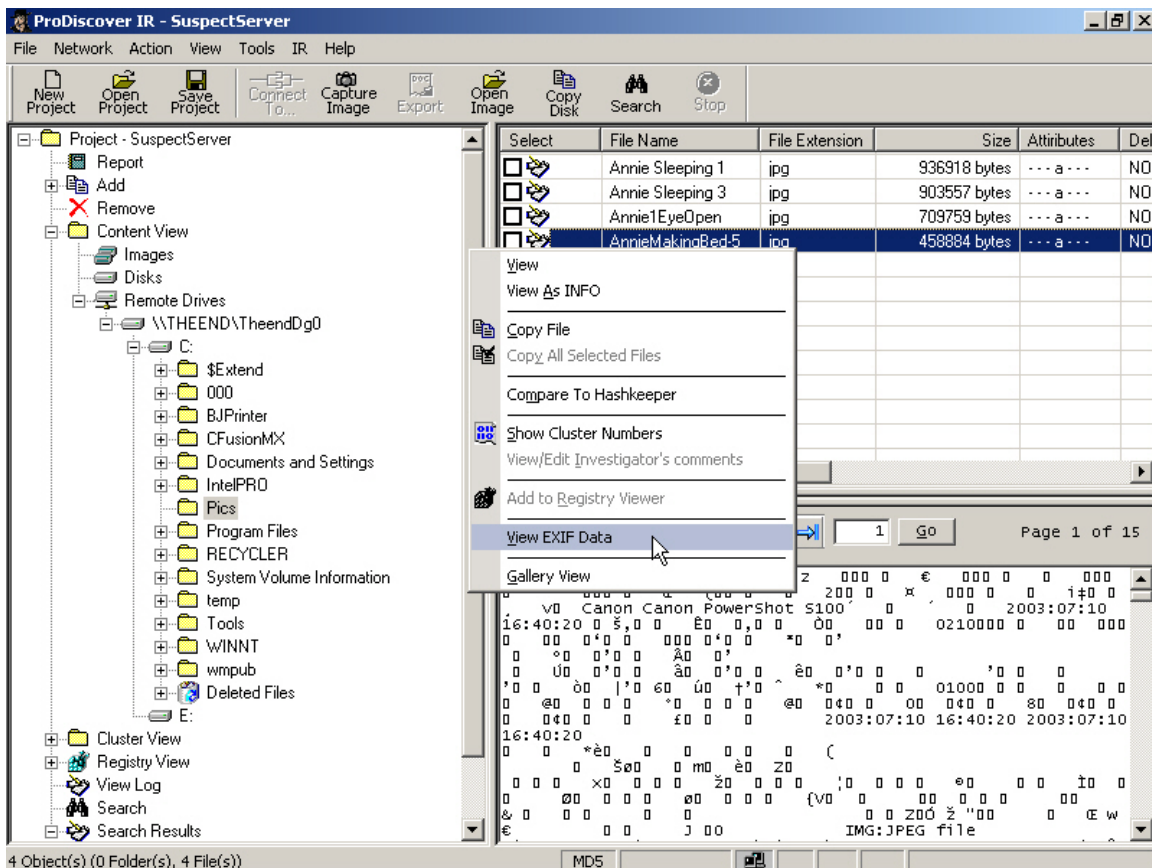


View Image EXIF Meta Data

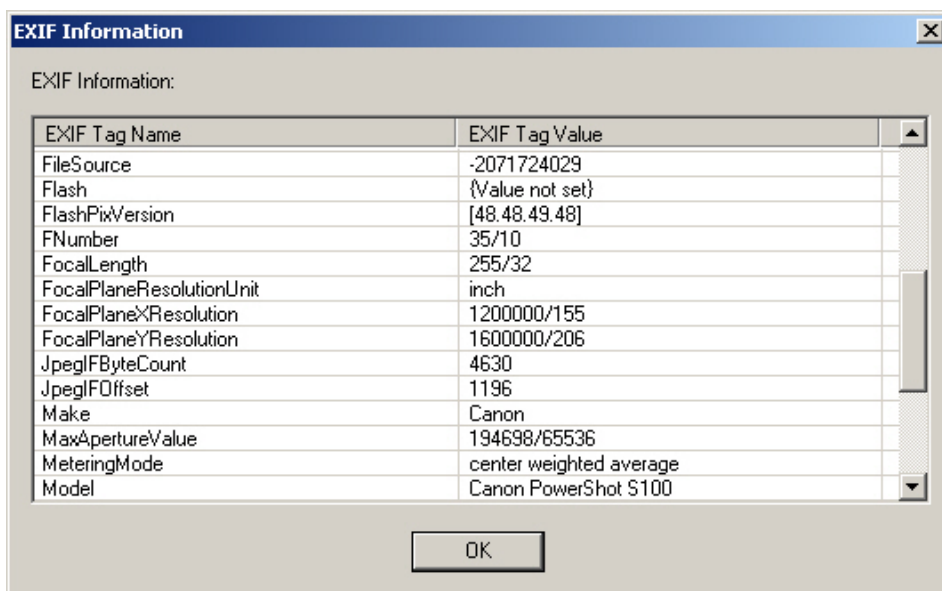
The Japanese Electronic Industry Development Association (JEIDA) created a standard for the storage of camera and image metadata in JPEG and TIFF files. Most digital camera manufacturers have implemented this standard and now store camera metadata along with the digital image. This metadata can potentially provide vital evidence to investigators such as when the picture was taken, what camera was used in capturing the image and in some cases, who took the image or where the image was captured.

The Tag tables in EXIF meta data provide a tremendous amount of potentially useful information if contained in the EXIF section of a JPEG file. While it is cumbersome to try to pull this data manually from the file, programs exist today to extract this data for the investigator. Programs such as EXIFutils or IMatch can be used to view this information. Technology Pathways forensic tool, ProDiscover will automatically extract and report this information for investigators if desired for all JPEG and TIFF files marked as evidence of interest. This can open up a whole new avenue for investigators and capture EXIF metadata in an evidentiary quality manner to be used in court at a latter date.

To view the EXIF meta data of a JPG or TIF file in ProDiscover simply right-click on any .jpg or .tif graphic file from content-view and select "View EXIF data" as seen below.



After choosing to view EXIF Data, users are shown a dialog box containing all available EXIF meta data as seen below.



In the user preferences "EXIF" tab, users have the ability to select if they want EXIF meta data added to the report when selecting (selected tag enabled) graphics files as evidence.

Recover a Deleted File

1. Ensure the desired evidence disk is connected to the ProDiscover system.
2. Select the **"Content View | Disk, or Image"** option from the Menu or tree-view.
3. ProDiscover displays a list of drives, or images available to the system.
4. Select the desired disk, or image and navigate to the desired volume.
5. ProDiscover displays the contents of the disk.
6. Select a file to recover from the work area.

Notes: The "Deleted" column will display "Yes" if the file has been deleted. On NTFS formatted drives, ProDiscover collects all deleted files into a special directory called "Deleted Files". The contents of a recovered file can never be guaranteed since some clusters may have been overwritten.
7. ProDiscover displays the contents of the selected file at the bottom of the main window.
8. **Right click** on a file.
9. ProDiscover a pop-up dialog with the choice to View or Recover the selected file. Select **Copy File**.
10. Enter the desired location and file name to save the file as in the "Save As" dialog box that appears and click **"Save"**.

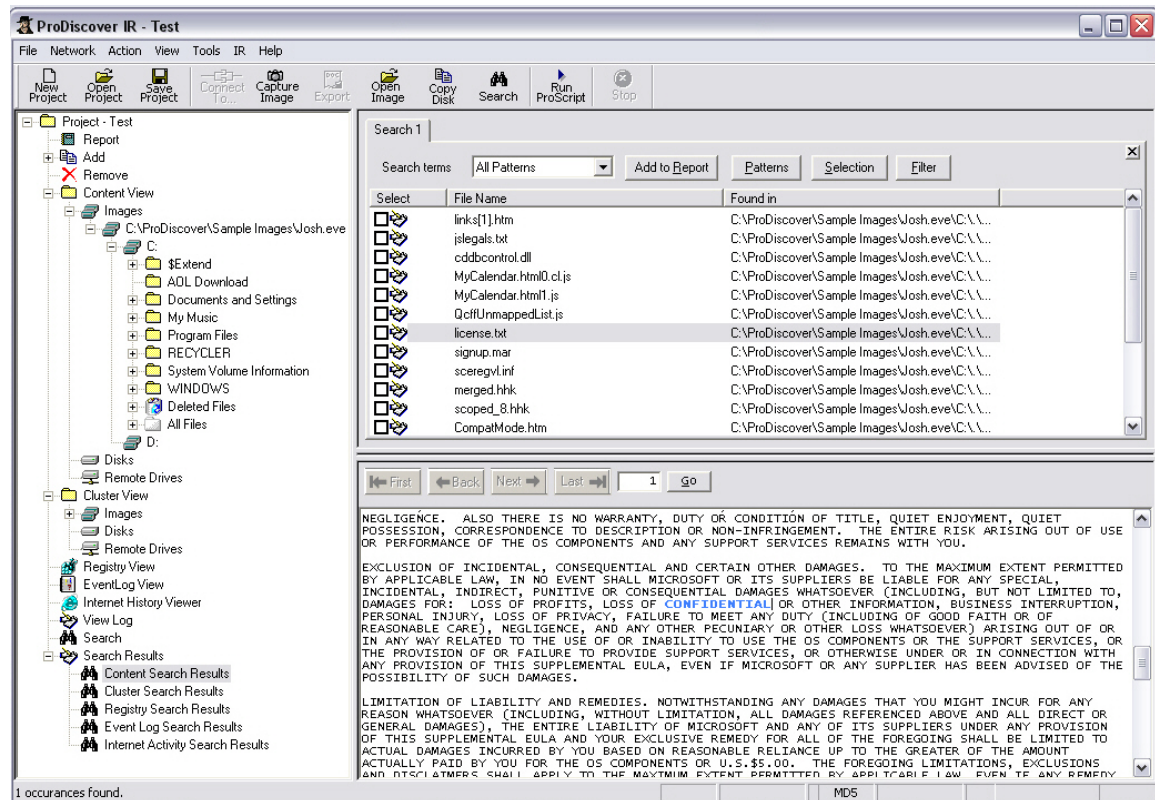
Search for key words in image file or disk

1. From the current project select search option from the tree-view, or button bar.
2. ProDiscover displays search dialog.



3. Choose the type of search to be conducted (Content or Cluster).
4. If conducting a content search choose "Search in Selected Files only" to search in only files selected as evidence if desired.
5. Checking the "Select all matches" checkbox will automatically add all files from the search result to the project report as evidence of interest. Files marked as evidence of interest can be easily copied to review disks using the ["copy selected files"](#) option from the tools menu.
6. If conducting a content search choose to search for file names or content.

7. Enter the keywords (one on each line) in the search for window and select the image files or disks to be searched. Full **Boolean Logic (AND, OR, NOT)** can be used, but must be capitalized. (See Appendix C for information on using Boolean Logic in search terms.) List of keywords can be saved in an ASCII text file with the extension .STS and loaded using the "Load from file..." button.
8. Users may also select to filter Content Searches by Modified, Accessed, or Created dates.
9. Click the "Search Now" button.
10. Results obtained from the search will be displayed in the top work area as selectable objects. When any object is highlighted the resulting search term will be highlighted in the data view area. Search results are saved from session to session in a file with the same project name and the extension .ds2
11. If the search results are satisfactory they can be added to the current projects report with the "Add to Report" button.

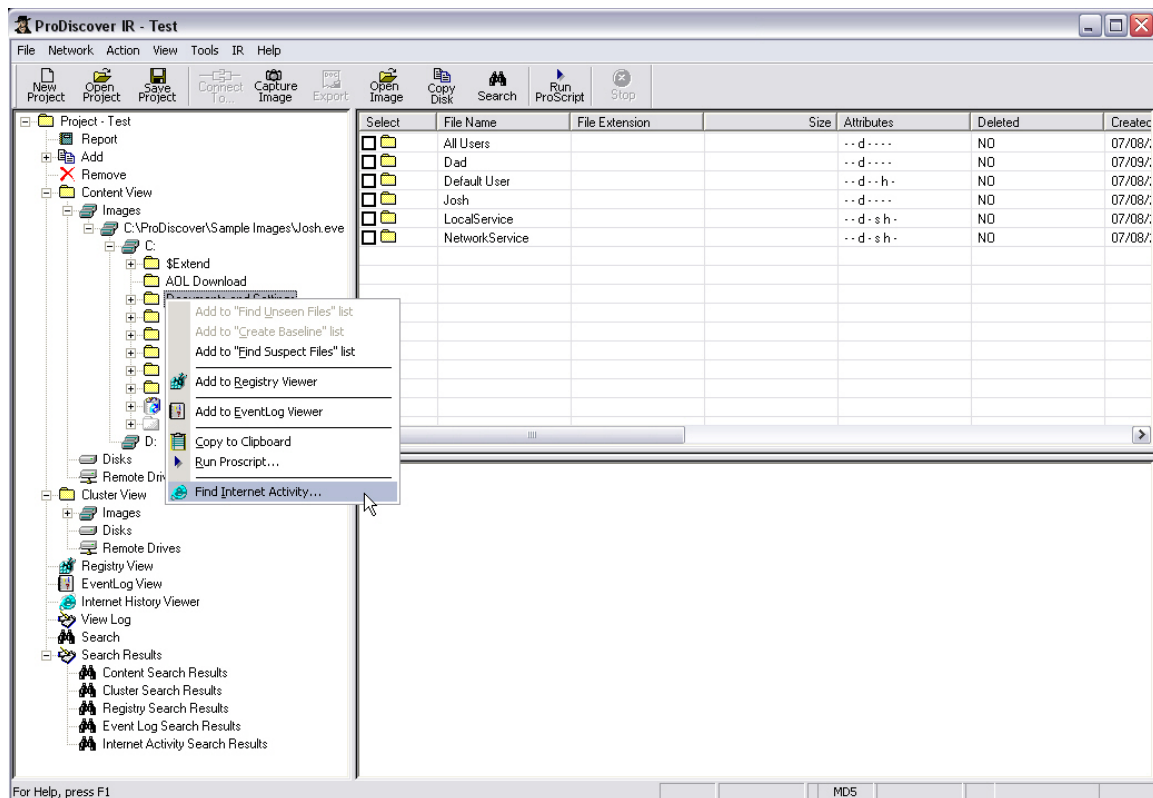


12. The "Search terms" drop-down box allows users to highlight only a single search term from the original search term list if desired.
13. The "Patterns" button will display a pop-up window containing the original search terms used in the search set including any Boolean operators used.

Extracting Internet History

Information about a users Internet Web surfing habits is often crucial to investigations. ProDiscover allows investigators to quickly search for, and extract information from Internet Explorer history files (index.dat). Once the information is extracted it is automatically added to the project report.

searching for and extracting the Internet history from a directly added disk or image is as simple as right-clicking on the desired directory structure and choosing "Find Internet Activity...". ProDiscover will then search the selected directory structure for all index.dat files containing Internet Explorer Web surfing history and populate the Internet History Viewer for further analysis and addition to the project report.

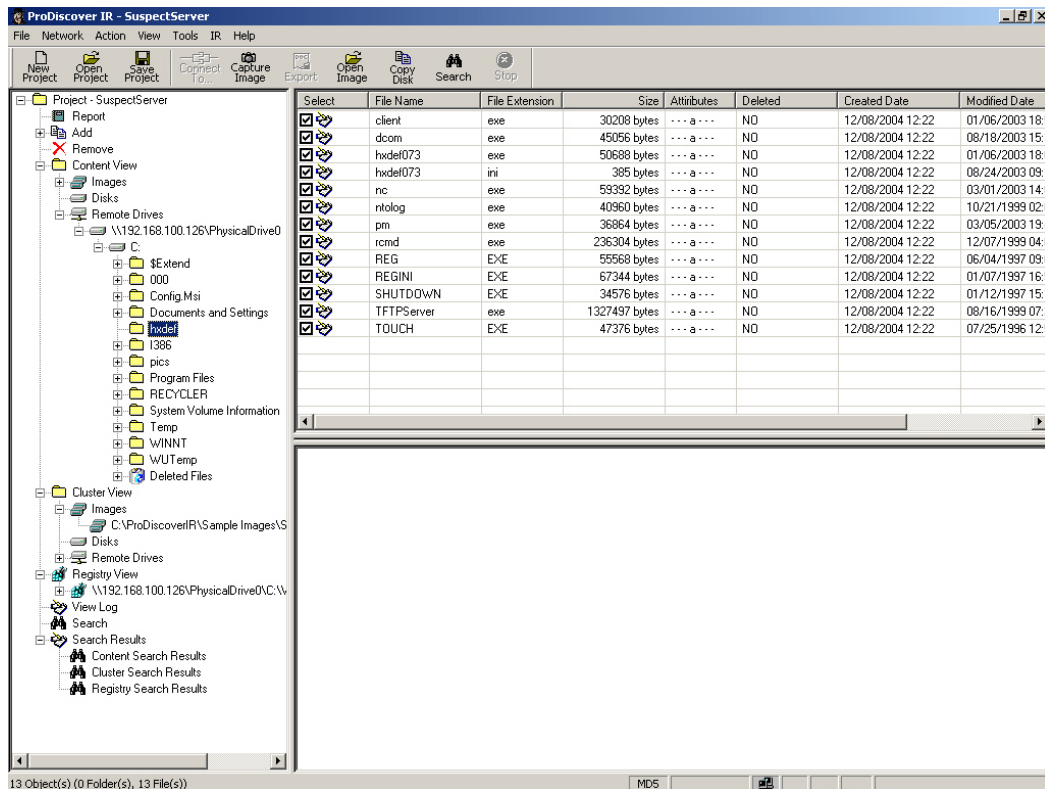


Once complete the Internet History Viewer found in the tree-view will be populated with the contents of each index.dat file created by Internet Explorer. Once added to the Internet History Viewer this information can be searched and added to the project report on an entry-by-entry basis.

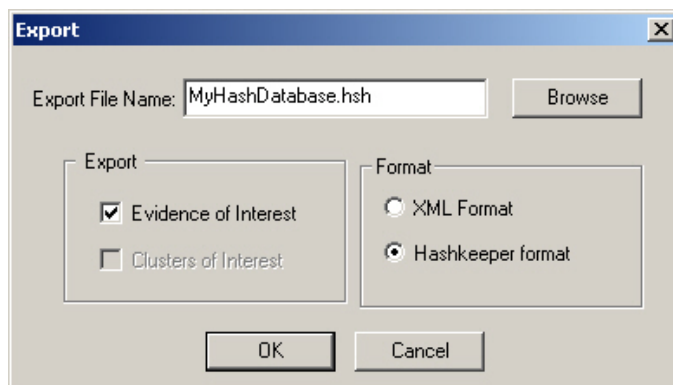
Creating Hash Database Files

Often users will want to create their own hash database files for use in cases. ProDiscover allows users to export file names and hash values of items selected as evidence of interest in the Hashkeeper *.HSH format for later use in hash comparison, filtering and the "Find Suspect Files" function found in ProDiscover Incident Response.

To create a hash database in the Hashkeeper *.HSH format, simply mark all desired files as evidence of interest by enabling the "selected" tab from content-view as seen below.



Once all items are marked selected, choose "Export Evidence of Interest" from the Action menu, ensure the "Hashkeeper format" radio button is selected and choose OK. The hashkeeper database will be exported to the selected file location and can be used by ProDiscover or other applications which use hashkeeper formatted databases.



Comparing HashKeeper hash sets

ProDiscover creates cryptographic checksums of “interesting files” in popular SHA1, SHA256, and MD5 algorithms. These checksums can then be compared to known file checksums maintained in the National Drug Intelligence Center (NDIC) Hashkeeper database. The HashKeeper is a database of known file hash values. The database uses the MD5 file signature algorithm to establish unique numeric identifiers (hash values) for known files and compares those known hash values against the hash values of unknown files on a seized computer system. Where those values match the examiner can say, with statistical certainty, that the unknown files on the seized system have been authenticated and therefore do not need to be examined. More information on HashKeeper can be found at www.hashkeeper.org.

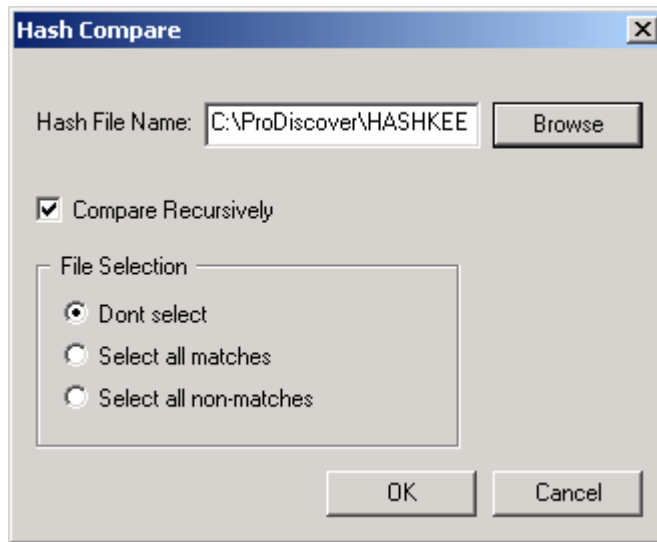
TIP:

"Filter by hash set" is a powerful feature which can also be used to identify files for which a hash is already known. Many investigators keep hash values in the hashkeeper format for files they often search for. See *the hashkeeper examples installed in the default program installation directory for the hashkeeper file format*. An example of this approach is creating a hash set of known rootkits or Trojans. Once the hash set is created "filter by hash set" can be used as a search mechanism to find the offending files.

Note that since MD5, SHA1, and SHA 256 file hashes are created for the contents of the file and NOT the file name, hash sets can be used to find known files even when the user has changed the file name.

To compare hash sets to a directory and all contents recursively:

1. Ensure the desired evidence disk is connected to the ProDiscover system and the desired disk has been added to the current project (or the desired image file has been captured and added to the project).
2. Select the **"Content View | Disks | Physical Drive | Partition"** option from the Menu or Tree-view.
3. Select the desired disk partition.
4. ProDiscover displays the contents of the disk.
5. Select a file or directory to compare.
6. Select the **"Tools | Filter by Hash Set"** option from the Menu.
7. Select the **"Tools | Filter by Hash Set | Highlight or Hide"** option from the Menu.
8. The **Highlight** option will highlight all files in blue that match a hash from the selected hashkeeper file. A **"k"** will also be added to all matching files attributes in the content view work area.
9. The **Hide** option will hide all files from view that match a hash from the selected hashkeeper file. Note that the number of hidden files can be viewed in the status bar.
10. Select the **"Tools | Filter by Hash Set | Hash File..."** option from the Menu.
11. ProDiscover displays a Popup window.



12. Select any exported HashKeeper hash file (Ensure the hash file extension is .hsh).
13. Choose "Browse".
14. Enable the "Compare Recursively" checkbox to compare all files and directories below the current folder if desired. Note: Recursive hashKeeper compare can take some time depending on variables such as: system configuration, amount of files, and size of hash file. As a benchmark a 40,000 file system compared against the entire HashKeeper database (45MB) on a 1.6 Ghz P 4 can take up to two hours.
15. The "File Selection" area allows the examiner to automatically select files as evidence of interest during the compare process. This feature is useful when using hashkeeper to find suspected files for which the user has a known set of hashes.
16. Choose "OK"
17. ProDiscover will take the action selected in number 7 above.

To compare hash sets to a single file:

1. Ensure the desired evidence disk is connected to the ProDiscover system and the desired disk has been added to the current project (or the desired image file has been captured and added to the project).
2. Select the "**Content View | Disks | Physical Drive | Partition**" option from the Menu or Tree-view.
3. Select the desired disk partition.
4. ProDiscover displays the contents of the disk.
5. Select a file to compare.
6. ProDiscover displays the contents of that file at the bottom of the main window.
7. Right click on the file to compare.
8. ProDiscover displays a Popup window.
9. Choose "**Compare to HashKeeper**".
10. Select a HashKeeper hash file (Ensure the hash file extension is .hsh).
11. Choose "**Open**".
12. ProDiscover will display the results.

Match File Signatures and File Extensions

On a windows systems a file signature identifying the type of file is normally contained in the first 20 bytes of the file. For example a Windows Bitmap file with the file extension .bmp would contain "424D" hexadecimal in the first 20 bytes.

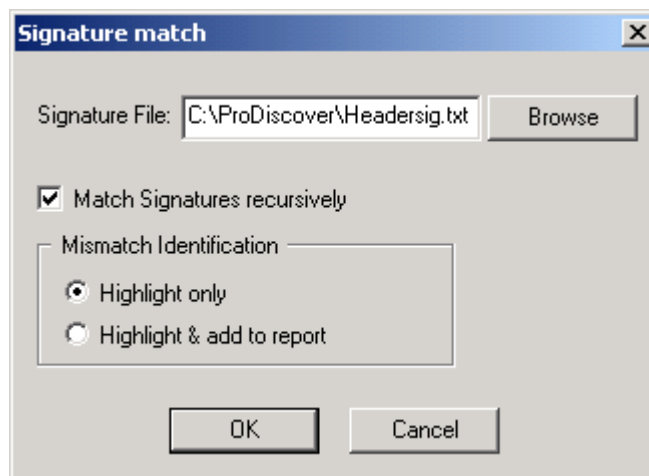
Note: The Hexadecimal numbering system, also known as base-16, describes a numbering system containing 16 sequential numbers as base units (including 0). The hexadecimal numbers are 0-9 followed by the letters A-F for the 11-16th positions.

File signature mismatch comparison can prove beneficial in filtering data as-well-as, uncovering rudimentary data hiding techniques.

See <http://www.filesig.co.uk/> for tools and resources for creating file signature databases for use in ProDiscover.

To match file signatures against file extensions within a directory and all contents recursively:

1. Ensure the desired evidence disk is connected to the ProDiscover system and the desired disk has been added to the current project (or the desired image file has been captured and added to the project).
2. Select the **"Content View | Disks | Physical Drive | Partition"** option from the Menu or Tree-view.
3. Select the desired disk partition.
4. ProDiscover displays the contents of the disk.
5. Select a file or directory to compare.
6. Select the **"Tools | Signature Matching"** option from the Menu.
7. ProDiscover displays a Popup window



8. Choose "Browse" to select any signature database file in the proper format. (See Appendix B - Signature Matching for the signature database format.)
9. Enable the "Match Signatures Recursively" checkbox to compare all files and directories below the current folder if desired. Note: Recursive Signature Match can take some time depending variables such as: system configuration, amount of files, and size of hash file.
10. The "Mismatch Identification" area allows the examiner options to highlight only, or highlight & add file signature mismatches to the current project report.
11. Choose "OK"
12. ProDiscover will take the actions selected within the dialog box settings.

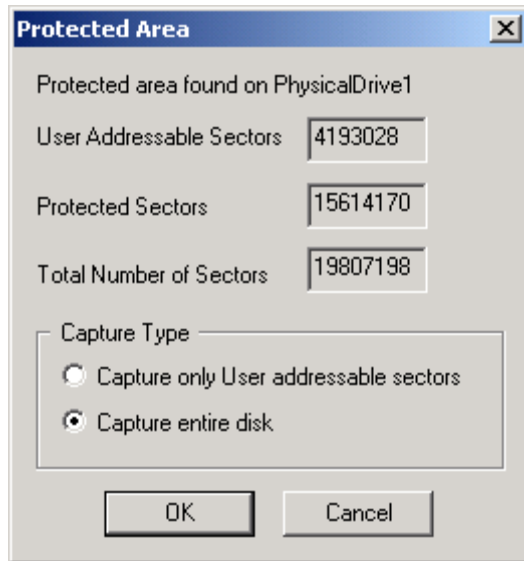
Detecting file systems within the HPA

1. Ensure the desired evidence drive is attached to the ProDiscover system.
2. Select capture image option from the action menu item, or button bar.
3. ProDiscover presents the capture image dialog.

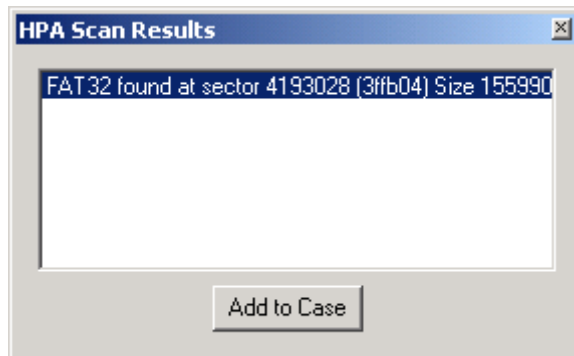
The screenshot shows the 'Capture Image' dialog box with the following fields and controls:

- Select Drive:** A dropdown menu showing 'PhysicalDrive1'.
- Destination:** A text field containing 'JonesDrive1' and a '>>' button to the right.
- Technician Name:** A text field containing 'Chris'.
- Image Number:** A text field containing '0023Q3'.
- Description:** A large text area containing 'Jones Home PC Drive 1'.
- Total sectors to capture:** A text field containing '19807198' and an 'HPA' button to its right.
- Compression:** A section with two radio buttons: 'Yes' (unselected) and 'No' (selected).
- Buttons:** 'Password', 'OK', and 'Cancel' buttons at the bottom.

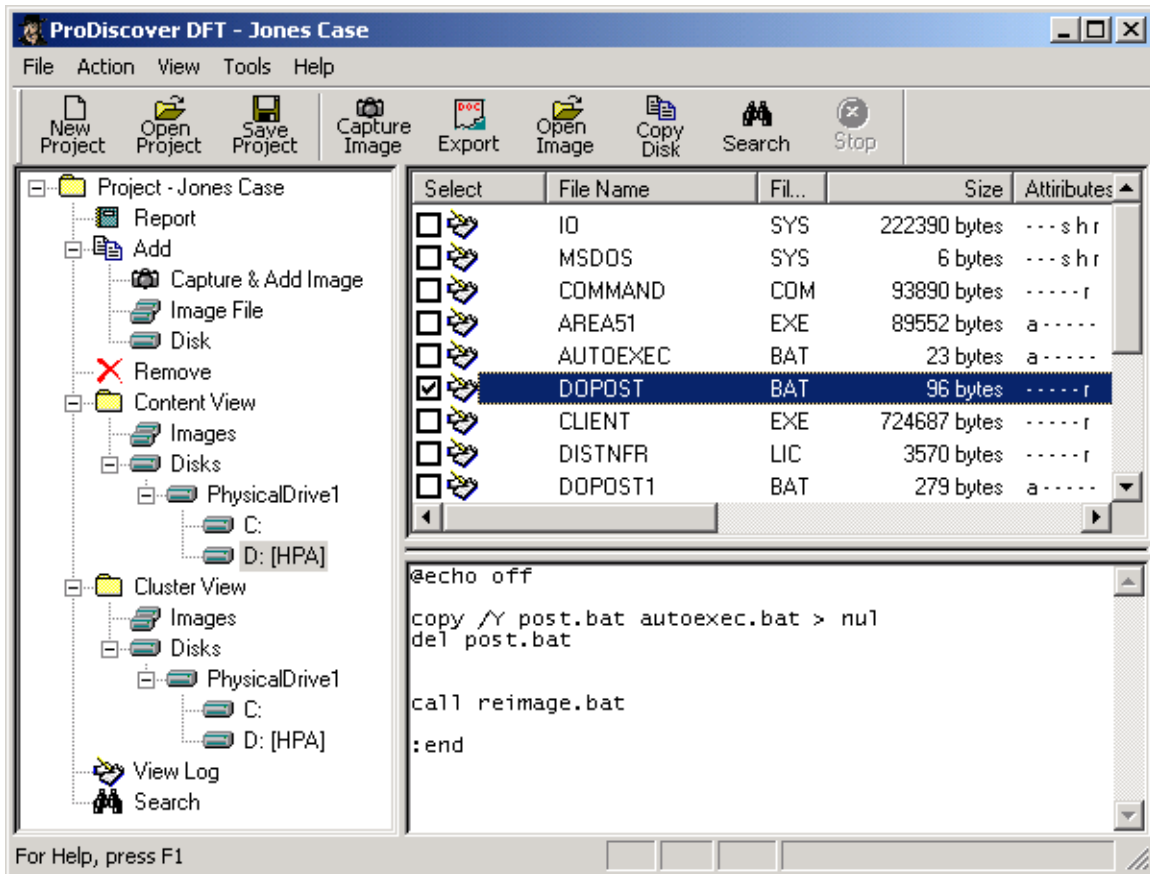
4. Select the drive to be captured, destination path for the image file to be saved into, compression and password protection of the image file and specify the technician name, image number, description of the image file.
5. If ProDiscover detects the image has a Hardware Protected Area the **"HPA"** button will be enabled. Selecting the button will display the following dialog allowing user control over the sectors to be imaged.



6. Ensure the HPA is detected and Capture entire disk is selected (default setting).
7. Click "OK".
8. ProDiscover reads the drive connected bit-by-bit and creates an image file in the specified location. The image file will contain an exact replica of the original disk, plus a few bites of checksum and log data.
9. Add the image file to the current project.
10. Click on "**Content View | Images | Image**"
11. Select "**Tools | Scan HPA**" from the menu bar.
12. If a file system was found within the HPA it will be displayed in the dialog that is displayed.



13. Choose "Add to Case" with the file system selected and ProDiscover will add the newly detected file system to the tree-view under the scanned image.

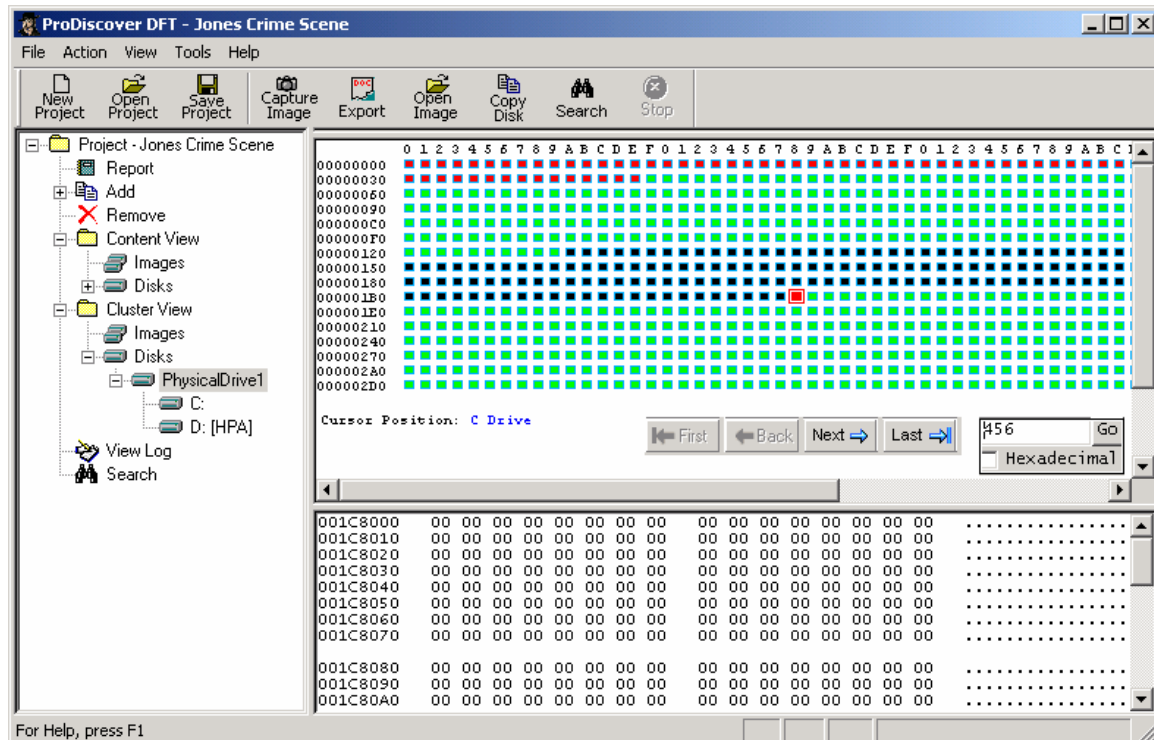


14. Work with the newly added partition in the same manner as any normal partition.

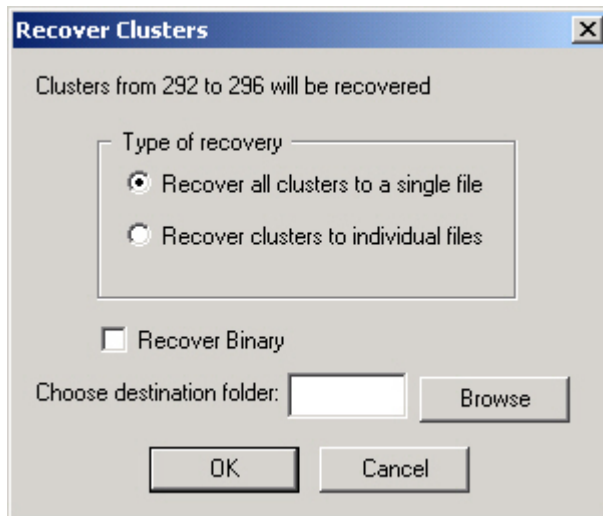
Recover a group of clusters

On many occasions an examiner will want to recover unallocated clusters or disk slack from evidence disk to a specified location. Recovering a cluster or group of clusters from Cluster View is as follows:

1. Ensure ProDiscover is running and a project is loaded.
2. Add an image or disk to the project.
3. Select "**Cluster View | Disks | Disk**" to bring up a cluster grid view in the work area as seen below.



4. click-and-drag from the desired starting cluster with the mouse button down to the desired ending cluster as seen above. Alternately users can use the shift-click method by holding down the shift button and clicking on individual clusters for recovery.
5. Right-click with the mouse cursor positioned above any of the selected clusters and select "**Recover Selected**".
6. A dialog box will pop-up asking for the type and location of recovery.



7. Choose single or multiple file recovery.

8. Enable the **"Binary"** checkbox to recover clusters as a binary file. Otherwise leave the checkbox unchecked to recover as ASCII text.

9. Choose file destination and click on **"OK"**.

[Note: users can also automatically extract clusters found in search operations.](#)

Detecting Disk or Image Installed OS

Information about the installed operating system of an evidence disk or image is sometimes critical to an investigation. To search an evidence disk or image for this information and add the data to a projects report take the following steps:

From within an active project with an evidence disk or image added select and highlight any partition from Content-View.

From the action menu select "OS Info".

ProDiscover will scan the selected partition for Windows registry files. Once the registry files are found they are parsed for Windows installation information.

The following Windows installation information is then extracted from the registry keys and appended to the current project report:

```
Installed Operating Systems Information
OS Found at Path: C:\WINDOWS
Registry keys:
InstallType = 01 00
SetupFlags = 0E 05 00 00
DevicePath = C:\WINDOWS\INF
ProductType = 1 1 1
RegisteredOwner = John Q. Suspect
RegisteredOrganization = Sample Company, Inc
ProductId = 52578-335-0238492-21585
LicensingInfo =
```

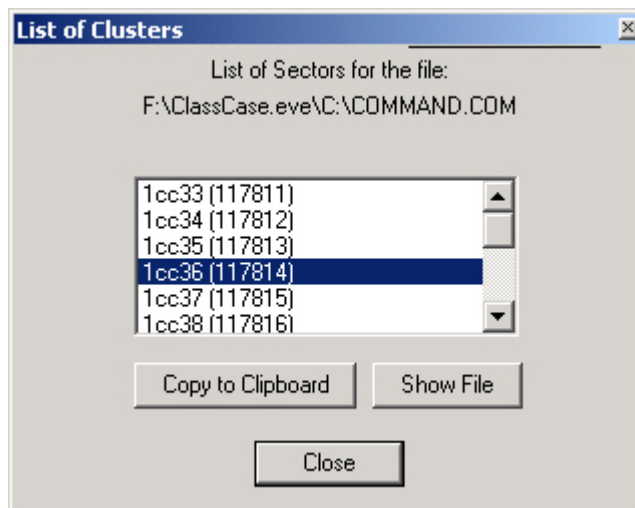
DVD_Region = 1
BPC_Region = 1
OldWinVer = 00 04
ProductKey = AD21J-AD7R7-T1JGD-323WM-32PVM
DigitalProductId = A4 00 00 00 03 00 00 00 35 30 34 37 38 2D 33 33 35 2D 30 32 30 38 37
39 32 2D 32 31 30 37 35 00 02 00 00 00 37 33 30 2E 30 30 38 34 37 00 00 00 00 00 00
00 80 63 EF 27 2C 69 46 3E 09 AA 87 D5 45 16 02 00 00 00 00 00 8F 51 DD 3D A9 37 03
00 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 30 30 34
30 30 00 00 00 00 00 00 00 00 00 00 00 00 D8 BB 80 54 00 01 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 C0 C8 28
1B
SubVersionNumber = A
ProgramFilesDir = C:\Program Files
CommonFilesDir = C:\Program Files\Common Files
Plus! VersionNumber = IE 5 6.0.2800.1106
WallPaperDir = C:\WINDOWS\Web\Wallpaper
MediaPath = C:\WINDOWS\media
ConfigPath = C:\WINDOWS\config
SystemRoot = C:\WINDOWS
OldWinDir =
ProductName = Microsoft Windows 98
HWID = 0
MSID = 0
RegistrationExtDLL = OEMREG.DLL
RegDone =
FirstInstallDateTime = (Wednesday, March 02, 2002)
Version = Windows 98
VersionNumber = 4.10.2222
BootCount = 3
ProgramFilesPath = C:\Program Files
SM_AccessoriesName = Accessories
PF_AccessoriesName = Accessories
OtherDevicePath = C:\WINDOWS\INF\OTHER
ChannelFolderName = Channels
CacheWriteDelay = 7D0

Cross Reference File Cluster Locations

In some situations users will want to cross reference specific file cluster locations by file or by cluster. This operation can be easily accomplished with the following steps.

To find a list of specific clusters in which a file is written:

1. Ensure the desired evidence disk is connected to the ProDiscover system.
2. Select the **"Content View | Disk, or Image"** option from the Menu or tree-view.
3. ProDiscover displays a list of drives, or images available to the system.
4. Select the desired disk, or image and navigate to the desired volume.
5. ProDiscover displays the contents of the disk.
6. Select a file to recover from the work area.
7. ProDiscover displays the contents of the selected file at the bottom of the main window.
8. **Right click** on a file.
9. ProDiscover displays a pop-up dialog with several choices including to "Show Cluster Numbers" of the selected file. Select **"Show Cluster Numbers"**.
10. A pop-up dialog will appear showing the clusters belonging to the selected file. Double-clicking on any individual cluster will change the program focus to **"Cluster-View"**,

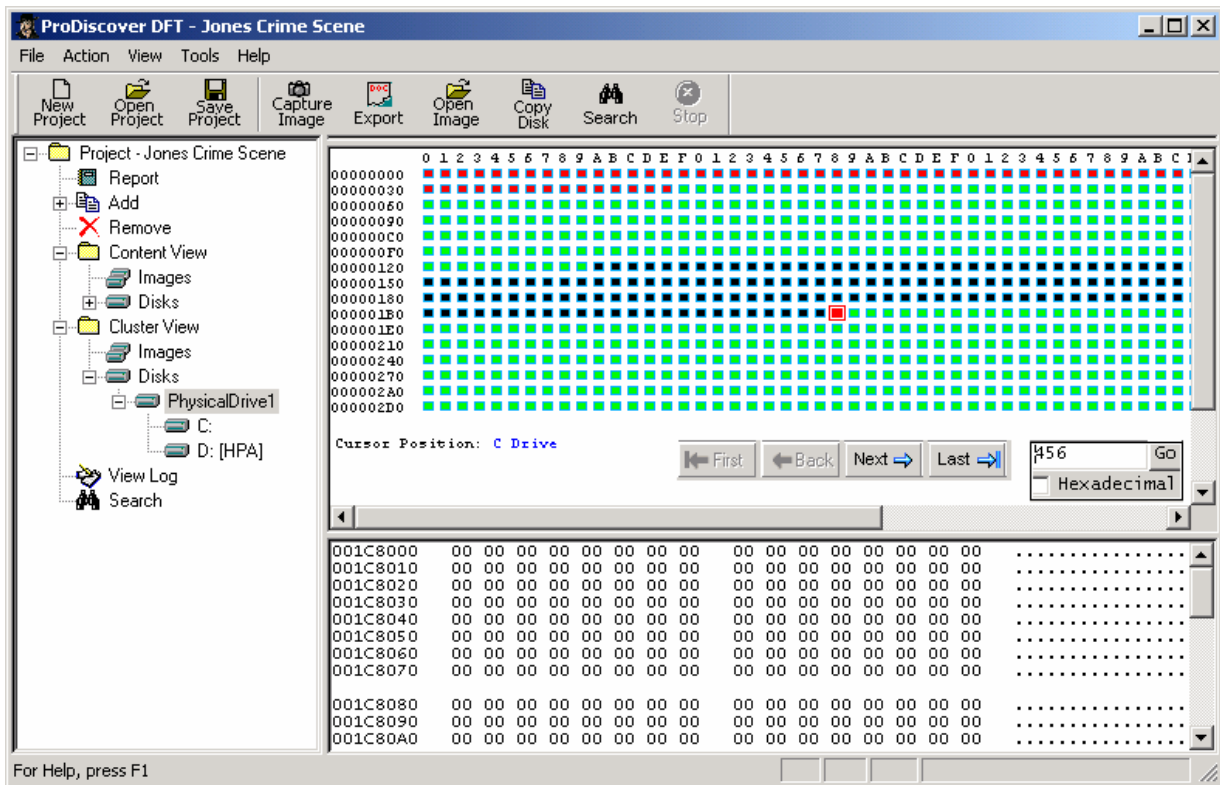


11. Selecting **"Show File"** will return program focus to the specific file in **"Content-View"**.
12. **"Copy to Clipboard"** allows the user to easily copy the cluster list and file information to the clipboard.

To find the file associated with a specific cluster:

On many occasions an examiner will want to recover unallocated clusters or disk slack from evidence disk to a specified location. Recovering a cluster or group of clusters from Cluster View is as follows:

1. Ensure ProDiscover is running with a project is loaded.
2. Add an image or disk to the project.
3. Select **"Cluster View | Disks | Disk"** to bring up a cluster grid view in the work area as seen below.

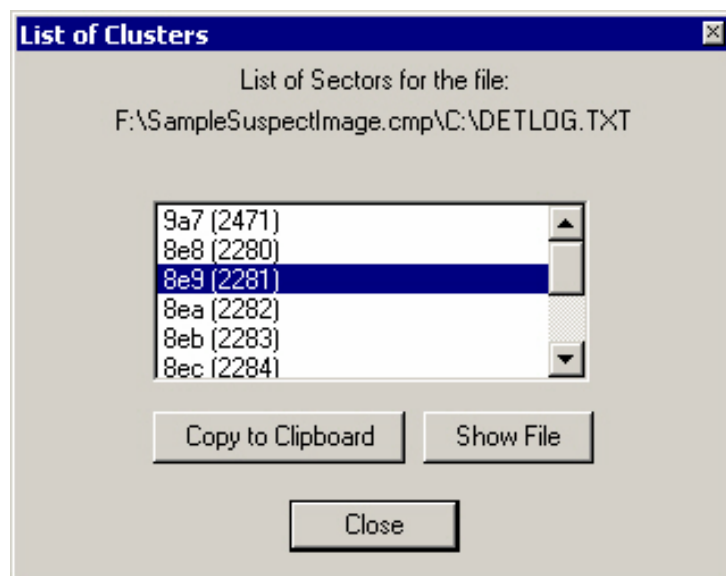


4. click any specific cluster with the mouse button to highlight the cluster.
5. Right-click with the mouse cursor positioned above the selected cluster and select **"Find File"**.
6. After searching the file system for the specific file which claims the cluster a dialog box will pop-up showing the file which the specific cluster belongs to along with other clusters which make up the specific file.
7. Click on "Show File" to change program focus to the specified file in **"Content-View"**.
8. Double-clicking the cluster number will return program focus to **"Cluster-View"**.

Determining and Cross Referencing a File's Cluster Locations

It is often helpful to know the specific cluster locations for individual files. ProDiscover allows users to easily find and navigate through any file's cluster locations.

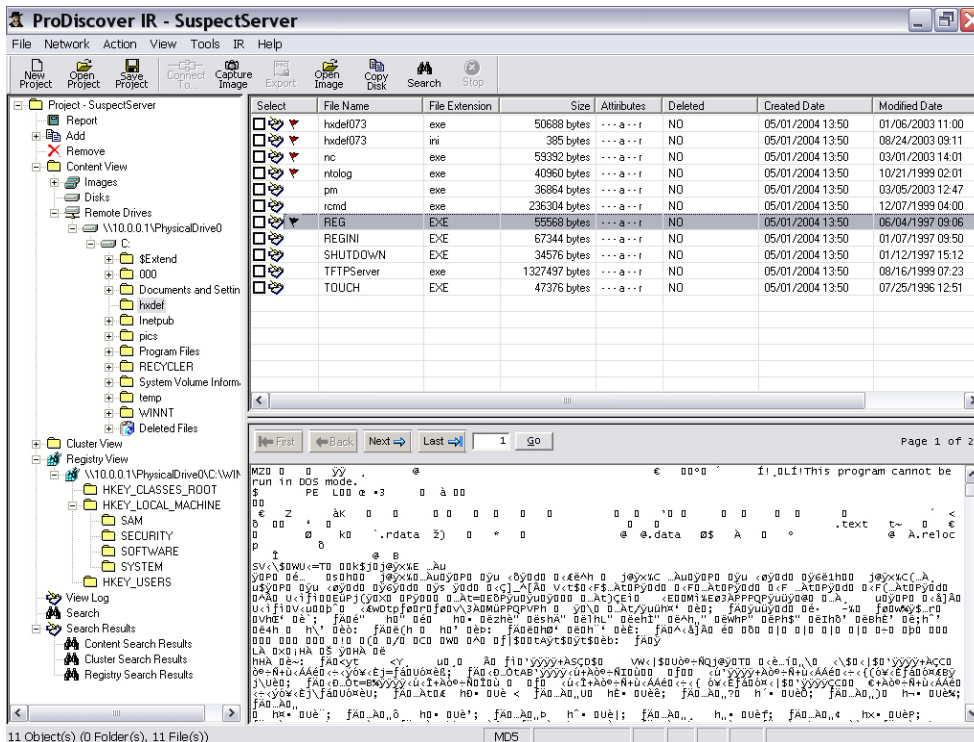
1. From Content-View right-click on any file.
2. Select **"Show Cluster Numbers"** from the pop-up menu.
3. The dialog box that appears will show all cluster locations (both hex and decimal) in which the file resides on disk.
4. Users can easily navigate to a specific cluster location in Cluster View by double-clicking on a specific cluster from the list-box.
5. To navigate back to the file location, choose the **"Show File"** button.
6. Conversely, right-clicking on a cluster from Cluster-View and selecting **"Find File"** will allow the user to find the specific file for the selected cluster.



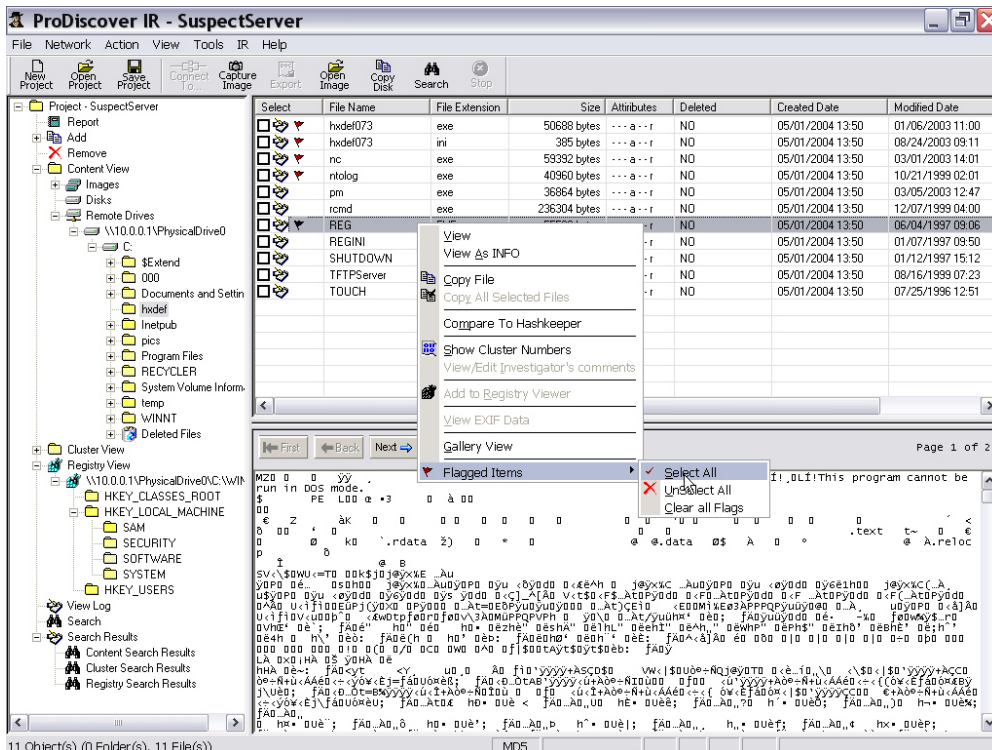
Flagging or Bookmarking Evidence of Interest

Often users will want to flag or bookmark items for later inclusion in the project report as evidence of interest. By **flagging** items prior to actual selection as evidence of interest users can operate much more quickly because the flagging operation does not incur the added overhead to create a cryptographic hash for the selected item. Flagging also allows users to make changes to what will become the final selection list during the investigation process.

To flag an item for later selection as evidence of interest users need only hold down the shift key and right-click over the item. Once the item is flagged it will show a red flag icon next to the file icon in the select column.

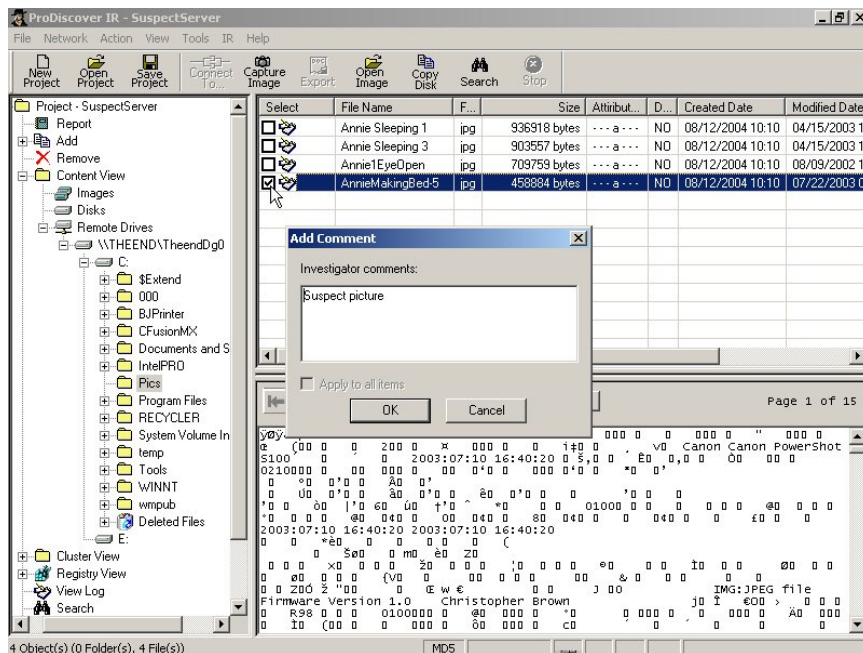


Once the user has all items flagged they desired for selection as evidence of interest the selection and hashing process can be accomplished by right-clicking over one of the flagged items and choosing "Flagged Items | Select All" from the pop-up menu as seen below. A pop-up dialog box will allow the user to apply investigator comments to each item individually or to the flagged group as a whole.



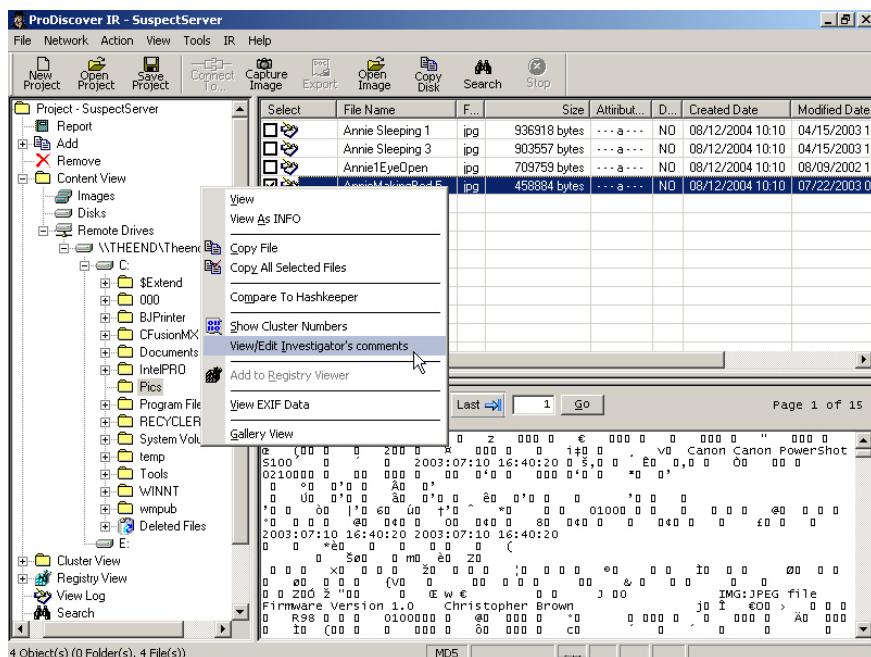
Adding and Editing Comments to Evidence of Interest

The ProDiscover report viewable from the left hand navigation tree is static until exported, however, users can add and edit comments on individual evidence of interest. When marking an item as evidence of interest by enabling the selected tag, users are automatically presented with a dialog box for entering comments as seen below.



Any comments added in the dialog box will be added to the report's evidence of interest section for that item. When selecting multiple items users are given the option to apply the same comment to all items selected.

Once an item is added as evidence of interest and the user desires to change the comments they can do so by using the right-click option "View/Edit Investigator's Comments" as seen below.

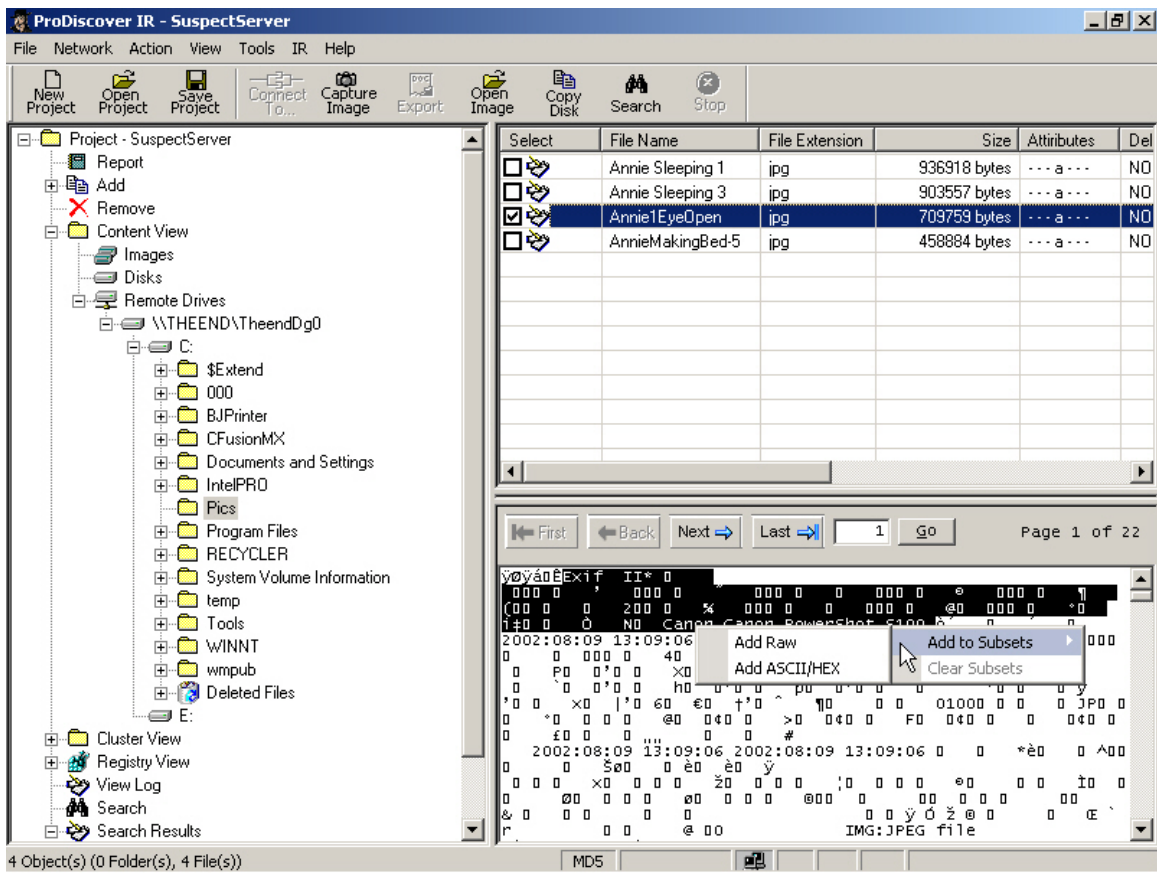


Adding Subsets of Data as Evidence of Interest

In some cases a user will want to add or highlight only a specific subset of information from a file as evidence of interest in the report. This feature is especially helpful when the specific item of interest is only a few words in a long document.

To add specific items of interest to the current project report users should "left-click and drag" across the specific data area from the data view area, then right click over the highlighted area and choose "Add to Subsets". Users will be given the further option to choose to add the data as Raw text or in a ASCII/HEX view. The described operation is illustrated below.

Note: If the user had not previously selected the item as evidence of interest, the item will then be marked "selected" as evidence of interest.



Using ProDiscover Remote Agent

Network Imaging & Analysis of Live Systems (ProDiscover Investigator and IR Version)

ProDiscover (*IR and IN* Versions) introduced the ability to perform live imaging and analysis of remote Windows™ based computers on TCP/IP networks. To accomplish remote imaging and analysis ProDiscover now consist of two components 1. the client which is where all standard ProDiscover functionality can be found and 2. the server (**PDServer**) which is run on any remote system users desire to image or conduct live analysis (often called preview).

ProDiscover offers the investigator several ways to get the PDServer remote agent running on the remote system.

- Investigators can have the remote agent pre-installed and password protected on the remote system.
- Investigators can simply insert the remote agent CD-ROM in the system to be investigated.
- Investigators can install the remote agent on other removable media devices such as thumb drives and floppy disks.
- The remote agent can be installed utilizing the remote installation batch scripts and utilities provided.
- Investigators can simply "push" the agent out and install using ProDiscover's Network | Install/Uninstall menu option. (This is the preferred method of installation and removal for many corporate investigators).

Note: Investigators should always use caution when working with live systems and use the least-intrusive method in remote agent execution available for the given situation. Understanding the changes made by their actions is imperative. Even when running the remote agent from CD-ROM on a live windows system, the live system will likely add the remote agent to the recently run applications list in the registry. While this is certainly a reasonable change in many situations the investigator should understand and document their actions. Reasonableness, understanding, and documentation are key factors for any investigator action during an investigation. Disk implementing whole disk encryption may only be able to be imaged live in order to obtain the evidence in an un-encrypted state.

Images of live remote systems are sometimes referred to as "smears" because rather than freezing the source remote image in time, bits on the remote system may change during the imaging process due to action on the system. During the imaging process of a live remote system each sector/bit on the system is read at the specific point in time and written to the corresponding sector/bit in the image file. This process essentially means that bit 0 in the image file was read at time "x" and bit 394 was read at time "y".

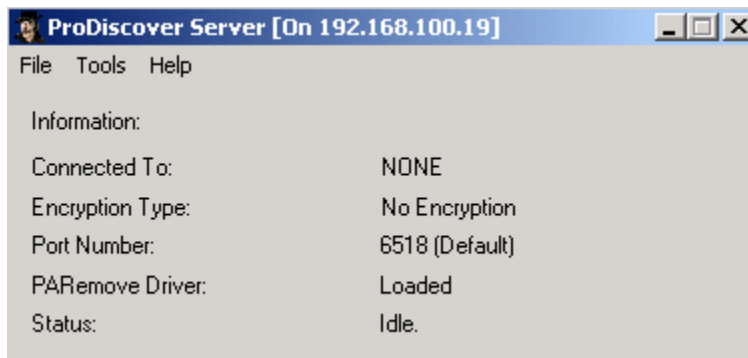
For investigators who wish to capture the disk at rest (offline) and thus not experience the effects of a smear, ProDiscover includes a Linux boot disk which has been modified to include only the minimum files necessary for Linux to run and join a TCP/IP network. This boot disk has the following features/capabilities:

- Auto discovers network adapters and allows for DHCP or Static IP Address assignment
- Includes and automatically runs the PDServer remote agent
- Will not mount or write to any physically attached disks
- Will not increment the Journal count on any journaling file systems such as Ext. 3

The PDServer Linux Boot Disk iso image can be found in the "Linux Boot Disk" folder off the default ProDiscover installation directory. Simply use your favorite CD burning software to create a new CD or use the one included in the ProDiscover box.

PDServer can be found in the "**Server**" sub-directory under the default ProDiscover installation directory. Users desiring to conduct live imaging or analysis of a remote Windows™ based system need only copy all the files located in the "**Server**" directory to a CD-ROM, Floppy Disk or USB Flash Disk and run **PDServer** on the remote system from the disk. Once **PDServer** is running on the remote system the standard ProDiscover client will be able to [connect to](#) the remote system and image, or add remote disks to the current project. In standard mode **PDServer** does not require a password for connection, imaging or analysis.

PDServer includes the ability to dynamically load the PARemove driver for remote detection, imaging and analysis of the Hardware Protected Area on Windows™ 2000 and Windows™ XP platforms. Dynamic loading of device drivers is not available in the Windows™ 98SE platform do to platform architecture. For more information on the Hardware Protected Area see [Advanced Tips and Tricks](#).



For users who desire to run **PDServer** for an extended period of time, or without the users knowledge **PDServer** offers two options for "**Stealth Mode**" found under the Tools menu.

PDServer Security

PDServer Remote Agent is designed to offer security and flexibility for remote acquisition and analysis. By default the PDServer Remote Agent is intended to be run from a trusted CD, USB Drive or floppy only during Incident Response or active Auditing. Users are provided the option to install the PDServer Remote Agent on systems in a "Stealth" mode, but this type of installation should not be left for extended periods of time. Technology Pathways has implemented the following PDServer Remote Agent security features to ensure data security and integrity:

Encryption

The user may elect to have all communications between the host and remote agent be protected by encrypting with 256 bit AES or Twofish encryption. Even if the user chooses to not enable encryption on the data, the password is always encrypted.

Secure Communication Protocol

The protocol used to establish a session and run all sessions to the remote agent employs Global Unique Identifiers (GUID's) to insure no other process can insert packets in the data stream. This insures the remote agent will only communicate to one client per session.

Password Protection

The remote agent is password protected to prevent use by unauthorized personnel. The password is always encrypted during the session establishment process, even if the user chooses not to encrypt the session.

Password Lockout

When the remote agent is set to require password authentication the agent will not accept logins for 5 min when an incorrect password is provided sequentially 5 times.

Write Protected Trusted Binaries

The remote agent is intended to be executed from a write protected device such as a CD or floppy so no unauthorized users may alter it.

Other Safeguards

Should the user elect to pre-install the remote agent, the code has been designed to be safe. The binaries are not capable of writing anything to the disk so a hacker cannot use it to create back-doors or load malicious code on the system. The code has been designed to not have any buffer overflow error conditions and we have not found any in our testing.

Creating a Windows PDServer Disk (ProDiscover IR & Investigator Version)

PDServer can be found in the "**Server**" sub-directory under the default ProDiscover installation directory. Users desiring to conduct live imaging or analysis of a remote Windows based system should copy PDServer.exe and All other files located in the "**Server**" directory to a CD-ROM, Floppy Disk or USB Flash Disk. Once the **PDServer** disk is created, place the disk in the target system and run PDServer.exe from any running Windows based system to conduct live imaging & analysis.

Files located in the "**Server**" sub-directory are not copy protected and do not require a license file, so users are free to create as many **PDServer** disks as they desire.

ProDiscover Investigator Version

Users of ProDiscover Investigator version will also find a \SServer directory which can be used to create a stealth-only cd containing SPDServer which will only run in the stealth mode.

Creating and Running the Sun Remote Agent

To use the Sun Remote Agent from CD simply use any CDROM burning software capable of creating a CD from an ISO image and burn a CDROM using the SunSparcPDServer.iso or SunX86PDServer.iso found in the \Server\Solaris\Sparc, or \Server\Solaris\x86 directory depending on your target platform.

Alternately a remote agent disk can be created by burning the following 4 files to CDROM:

```
libstdc++.so.5
libstdc++.so.5.0.5
libgcc_s.so.1
PDServer
```

If the Libgcc and Libstdc++ libraries are not currently installed on the system running the remote agent the library search path may need to be modified to search the current directory. Adding the following two lines to the current profile will modify the search path to include the current directory.

```
LD_LIBRARY_PATH=./:$LD_LIBRARY_PATH
export LD_LIBRARY_PATH
```

When installing and running PDServer from files installed on the remote system the file libstdc++.so.5 can be deleted and a symbolic link can be created using the following command:

```
In -s libstdc++.so.5.0.5 libstdc++.so.5
```

Creating a Linux PDServer Disk

To use the Linux Remote Agent from CD simply use any CDROM burning software capable of creating a CD from an ISO image and burn a CDROM using the LinuxPDServer.iso found in the \Server\Linux directory.

Alternately a remote agent disk can be created by unarchiving and burning the following file to CDROM:

Server\Linux\PDServer<_Version>.tar

Creating a PDServer Linux Boot Disk

ProDiscover includes an iso image of a Linux boot disk which has been modified to include only the minimum files necessary for Linux to run and join a TCP/IP network.

This boot disk has the following features/capabilities:

- Auto discovers network adapters and allows for DHCP or Static IP Address assignment
- Includes and automatically runs the PDServer remote agent
- Will not mount or write to any physically attached disks
- Will not increment the Journal count on any journaling file systems such as Ext. 3

The PDServer Linux Boot Disk iso image can be found in the "Linux Boot Disk" folder off the default ProDiscover installation directory. Simply use your favorite CD burning software to create a new CD or use the one included in the ProDiscover box.

PDServer in Stealth Mode (ProDiscover IR & Investigator Version)

For users who desire to run **PDServer** for an extended period of time, or without the users knowledge **PDServer** offers two options for "**Stealth Mode**" found under the Tools menu.

Install Stealth Mode (Automated Installation)

The preferred method of installing the remote agent for many investigators is through the "Network | Install/Uninstall PDServer" menu option. Through this menu option investigators can easily set the install, uninstall, choose installation type, and remote agent settings such as the process name, port and password. If the investigator does not have the proper privileges to install the remote agent on the target machine, a dialog box will appear allowing a user name and password with the proper privileges to be entered.

Note: All installations using the "Network | Install/Uninstall PDServer" menu option are installed in Stealth mode only.

Install/Uninstall PDServer on Remote Machine

Enter computer name or IP address: 192.168.100.122

☒ Install PDServer on remote system
☐ Uninstall PDServer from remote system

Installation Type

☒ Install as a Service
☐ Install in Windows Run Registry Key

PDServer settings

Executable Name: PDServer.exe

Default Port: 6518

Password:

Re-enter password:

OK Cancel

Choosing to install in "Windows Run Registry Key" causes the remote agent to only run while a user is logged on to the remote system. The specific entry can be found in HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

PDServer.exe /E:xxxx (where xxxx is the encrypted version of the password (up to 19 characters) set by the user)

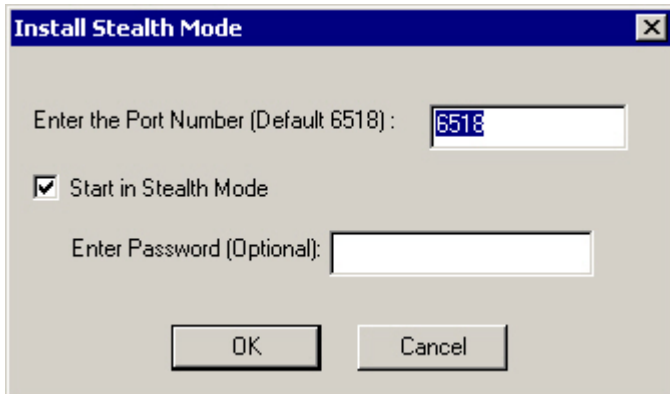
Once the user presses "OK" ProDiscover will install the Remote Agent and support files in the system32 directory of the target machine. Files installed include:

- Disk16.dll
- Disk32.dll
- msvcrt.dll
- PDServer.exe
- DFTSrv.exe (Installed only if installing as a service)
- DFTSrv.ini (Installed only if installing as a service)

If the user selects to uninstall PDServer from the remote system, all the above files will be removed with the exception of "msvcrt.dll" because other installed applications may depend on this file. Additionally any prefetch entries for PDServer.exe-pf and DftSrv.exe-pf will also be removed.

Install Stealth Mode (Manual Installation)

To use "Install Stealth Mode" all the files from the **PDServer** disk should be copied to a directory on the target computer. Once all files have been copied run **PDServer**, then select "Install Stealth Mode" from the tools menu to launch the installation dialog box. The user may change the **PDServer** default TCP/IP port and select the "Start in Stealth Mode" checkbox to ensure **PDServer** is not visible to users on the target system. Optionally a password can be set requiring any ProDiscover client to provide the password upon connection. Even when encryption mode is not set the initial connection setup and password communications are encrypted to prevent man-in-the-middle attacks.



Choosing OK will make the following registry entry on the target system.

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

PDServer.exe /s:xxxx (where xxxx is a password up to 19 characters)

Removing all the **PDServer** files and this registry entry is all that is needed to completely remote **PDServer** from the target system.

Switch to Stealth Mode

Runs **PDServer** without visibility on the program bar or tray area.

PDServer Command Line Options

1. **PDServer** can be started in stealth mode from the command line with:

"PDServer.exe /s:xxxx" (where xxxx is a password up to 19 characters)

2. **PDServer** can be launched from the command line with a specified TCP/IP Port number with:

"PDServer.exe /p:xxxx" (where xxxx is the desired port number)

Stealth Only Remote Agent (ProDiscover Investigator and Incident Response only)

In cases where investigators are concerned with the PDServer Remote Agent only running in Stealth mode, Technology Pathways provides a version of PDServer called "SPDServer.exe" which is only capable of running in the stealth mode. This version of the Remote agent prevents the investigator from accidentally running the agent in a mode where it is visible in the foreground by the end user.

SPDServer can be found in the \SServer directory of ProDiscover Incident Response and Investigator Versions. To use SPDServer in scripts simply backup the normal version of PDServer found in the \Scripts directory, rename SPDServer.exe to PDServer.exe and place the new file in the \scripts directory. Users who wish to auto-run the Stealth Only version of the Remote Agent can burn the contents of the \SServer to a CDROM.

Using the PDServer Linux Boot Disk

ProDiscover includes a Linux Boot Disk which will boot a stripped down version of the Linux operating system from CD-ROM containing the Linux PDServer Remote Agent. During startup the PDServer Linux Boot Disk will:

- Boot a Striped down Version of the Linux Operating System.
- Load detected network drivers including wireless cards
- Allow for manual or automatic configuration of IP Address.
- Automatically run the linux version of PDServer.
- Allow connections to the default PDServer port 6518.

The PDServer Linux Boot Disk is useful for investigators who desire a static image over the network or via a crossover cable. The PDServer Linux Boot Disk can be helpful to image disks in situations where the physical disk may be difficult to remove, access or that is device locked to run only in specific hardware.

ProDiscover includes an iso image of a Linux boot disk which has been modified to include only the minimum files necessary for Linux to run and join a TCP/IP network. The Linux boot disk had been modified to:

- Not mount or write to any physically attached disks
- Not increment the Journal count on any journaling file systems such as Ext. 3

The PDServer Linux Boot Disk is provided in CD-ROM format in packaged versions of ProDiscover Investigator and Incident Response. An iso image of the PDServer Linux Boot Disk can also be found in the "Linux Boot Disk" folder off the default ProDiscover installation directory. Simply use your favorite CD burning software to create a new CD or use the one included in the ProDiscover box.

ProDiscover & PDServer Remote Agent Firewall Configuration

This section describes how the ProDiscover IR & PDServer™ remote agent network communication system works with an organization's existing firewall security. You will learn about ProDiscover requirements for TCP connections, as well as the IP ports needed to establish a connection between ProDiscover & PDServer™.

Components of a Secured Network System

A firewall is not necessarily a product, but a set of security mechanisms that an organization implements, both logically and physically, to prevent unsecured access to an internal network. Firewall configurations vary from organization to organization. Most often, the firewall consists of several components, which can include a combination of the following:

Routers

Proxy servers

Host computers

Application Gateways

Network Address Translation Gateways

Network Layers

Very rarely is a firewall a single component, although a number of commercial firewall companies attempt to put all of the components into a single product.

For most organizations, the firewall begins at the border or Internet connection point. The firewall identifies itself to the outside network as a number of Internet Protocol (IP) addresses, or as capable of routing to a number of IP addresses, all associated with Domain Name Service (DNS) names. The firewall might respond as a host, resulting in a virtual computer, or pass packets directly to an internal host.

ProDiscover and Firewalls

You can configure firewall components in a variety of ways, depending on your organization's specific security needs, policies and overall operations. While most firewalls are capable of allowing all outbound communications to occur transparently, they might be configured to support only specific connections based on security considerations. For example, some firewalls allow only primary TCP connections, which are considered the most secure and reliable.

For ProDiscover IR & PDServer™ to function properly your firewall only needs to pass TCP connections on assigned ports as described below.

Establishing a Connection with PDServer™ through a Firewall

When you use ProDiscover through LAN, WANs or over the Internet, only one IP port is required to establish the connection at each end (ProDiscover IR and PDServer™). The following table shows the port, its function, and the resulting connection.

Port	Function	Connection Transport
6518	Remote Data Stream	TCP

If a firewall is placed between the ProDiscover IR consol and PDServer™ remote agent, it must be configured so that inbound and outbound connections to the IP port listed above are not blocked. Both ProDiscover IR consol and PDServer™ use the same port for communications.

Firewall Limitations

Some firewalling methods such as proxy servers and outbound connection filtering present a challenge for application delivery. Secure network engineering and design presents a challenge to balancing usability and security. To help in achieving balance ProDiscover IR fully supports the SOCKS proxy standard and other application proxies such as, Microsoft's Winsock Proxy. Some firewalls are capable of accepting only

certain protocols and cannot handle transparent TCP connections. For example, if your firewall is a Web proxy server with no generic connection handling mechanism, you will not be able to use the ProDiscover IR application delivery through the firewall. Technology Pathways is aware of the need to support as varied a network topology as possible and is continually evaluating supplementary and alternative methods for ProDiscover IR.

Security and Policy Concerns

Some organizations might have security or policy concerns that require them to limit firewall configuration changes related to opening ports. These concerns might be based on network capacity planning or low confidence in the firewall technology being used. For situations where ProDiscover's specific port cannot be opened, the port for both ProDiscover console and PDServer™ remote agent can be manually changed to a port that may already be open such as the web server port (80).

The PDServer™ port can be changed using the command line option "/p:"

Example: <PDServer.exe /p:80> (where 80 is the desired port number)

The ProDiscover IR console port number can be changed using the Preferences dialog box from the **File** Menu.

Note that in a few highly secure environments the firewall may actually look inside a packet to ensure that the expected header information is present for a given port. In such cases the firewall would look inside the ProDiscover packet on port 80 (if port 80 was selected) and not see web server traffic and thus block the packet. For highly secure environments such as these a specific port would need to be allowed in the firewall configuration for the ProDiscover IR console and PDServer™ remote agent.

PDServer™ Remote Installation and Removal Scripts

In cases where customers use ProDiscover IR to remotely audit and monitor systems which are not easily accessible, it is sometimes a challenge to install and run the PDSEVER Remote Agent. To assist users that require this capability, Technology Pathways provides the PDServer™ Remote Agent installation and removal scripts.

The PDServer™ Remote Agent installation and removal scripts (batch files) automate the process of pushing the PDServer™ Remote Agent and support files out to systems you wish to examine, and later removing them from these systems.

Note: Additional files are required for these scripts to run. Read below for download instructions and file list.

Warning: The included installation and removal scripts remotely edit system registry. Modifying the included scripts or using remote Windows Registry Editors incorrectly can cause serious problems that could require you to reinstall your operating system or cause data loss.

Two Sets of remote installation and removal scripts are provided to support different types of installation. The script “**PDServerInstall.bat**” is useful when users desire to install PDServer and have the agent only run when a user is logged into the system. The script “**PDServerRemove.bat**” is designed to remove previous PDServer installations with the previous script. These are the only scripts supported when pushing the remote agent out to Win9x systems.

For users who wish to have PDServer pushed out to a remote system where the agent is immediately running as a windows service the script “**InstallAsService.bat**” is provided. The benefit of this installation is an investigator can connect to the remote system immediately whether a user is logged into the remote system or not. The name of the installed service will be “**Windows**” allowing users to utilize the windows “services” MMC Snap-in to remotely start and stop the service as desired. For removing the remote agent when installed in this manner the script “**RemoveService.bat**” is provided.

The command line parameters for running both sets of scripts are identical.

The installation script (PDServerInstall.bat) will allow you to:

1. Push PDServer™ and the support files out to a remote Windows NT, 2000 or XP system.
2. As a measure to help assist the effectiveness of running the PDServer™ Remote Agent in Stealth Mode on the system to be examined, the script allows users to rename PDServer.exe on the remote system.
3. Set PDServer™ to run in stealth mode with a password assigned.
4. Set the desired PDServer™ TCP/IP port number.
5. Make required run registry entries to start PDServer™ the next time a user logs into the remote system. Entries are made to the following remote system registry key;
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
6. After installation users can remotely run PDServer™ for the first time using any remote administration tool which allows remote command execution such as telnet or Hyena from Adkins Resource (<http://www.adkins-resource.com/>).

The removal script (PDServerRemove.bat) will allow you to:

1. Stop the PDServer™ Remote Agent process from running on the remote system.
2. Delete the PDServer™ Remote Agent and support files from the remote system.
3. Remove the PDServer™ registry key from;

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

Requirements:

1. To run these scripts successfully the user must have administrative rights on the target machine.
2. Both scripts require several files from the “Windows NT Server 4.0 Resource Kit” which must be obtained from Microsoft. The required resource kit files are; reg.exe, regini.exe, sc.exe, srvany.exe, instsrv.exe, OEMNSVRC.INF and now.exe
3. The “Windows NT Server 4.0 & 2000 Resource Kit” can be downloaded from the Microsoft web site at: <http://www.microsoft.com/ntserver/nts/downloads/recommended/ntkit/default.asp>
4. The removal script requires PSkill from the System Internals web site.
5. PSkill can be downloaded from the System Internals web site at: <http://www.sysinternals.com/ntw2k/freeware/pskill.shtml>

The following table list Required files used by the remote installation and removal scripts which are available from Microsoft Windows Server Resource Kit's and System Internals Web Site. If you have any difficulty obtaining these files please contact Technology Pathways technical support.

File Name	Date	Time	Size
instsrv.exe	04/18/2003	06:05 PM	32,256
now.exe	04/18/2003	06:06 PM	32,256
pskill.exe	02/24/2000	01:52 AM	77,824
rcmd.exe	12/02/1999	01:54 PM	20,480
rcmdsvc.exe	12/02/1999	01:54 PM	41,472
reg.exe	08/29/2002	04:41 AM	48,128
regini.exe	04/18/2003	06:07 PM	36,864
sc.exe	08/23/2001	06:00 AM	31,232
srvany.exe	04/18/2003	06:06 PM	8,192

How to run the installation script:

1. Download the required files described above from Microsoft and copy them to the “Scripts” sub-directory found under the ProDiscover installation directory.
2. Open up a command prompt and change directory focus to the “Scripts” sub-directory found under the ProDiscover installation directory.

Example:

- a. To install PDServer™ on a remote computer with the IP address 10.0.0.5, and disguise PDServer™ as msspoll.exe with a password of “jones” and running on the TCP/IP Port number 80 just type;
PDServerInstall 10.0.0.5 msspool jones 80
 - b. An installation log file will be created in the “Scripts” directory documenting the installation. The installation log file will include Installation IP address, service name, password and port for future reference.
3. After PDServer™ is installed on the remote system the service will automatically run the next time a user logs on to the system. To run the PDServer™ process installed in the example above immediately the command “**msspool /s:jones /p:80**” must be executed remotely using any desired remote administration application such as **telnet** which supports remote command execution. On Windows 2000 and XP systems a telnet server is installed, but not started by default.
 - a. To start the remote telnet server on a Windows 2000/XP system use the services application found in “Administrative Tools” to connect to the remote system. Once connected to the remote systems, right-click on the **telnet** service and choose **start**.

- b. Once the service is started open a local command prompt and type “telnet 10.0.0.5”
Where 10.0.0.5 is the IP address of the remote system.
 - c. Once logged into the remote system type “**msspool /s:jones /p:80**” if the using the installation example above.
4. The PDServer™ is now running in stealth mode and ready to be connected to from your ProDiscover IR consol system.

How to run the removal script:

1. Download the required files described above from Microsoft and copy them to the “Scripts” sub-directory found under the ProDiscover installation directory.
2. Open up a command prompt and change directory focus to the “Scripts” sub-directory found under the ProDiscover installation directory.

Example:

- a. To remove PDServer™ from a remote computer with the IP address 10.0.0.5, where PDServer™ was installed as msspool.exe just type;
PDServerRemove 10.0.0.5 msspool
- b. A removal log file will be created in the “Scripts” directory documenting the removal.

Troubleshooting PDServer Connection Problems

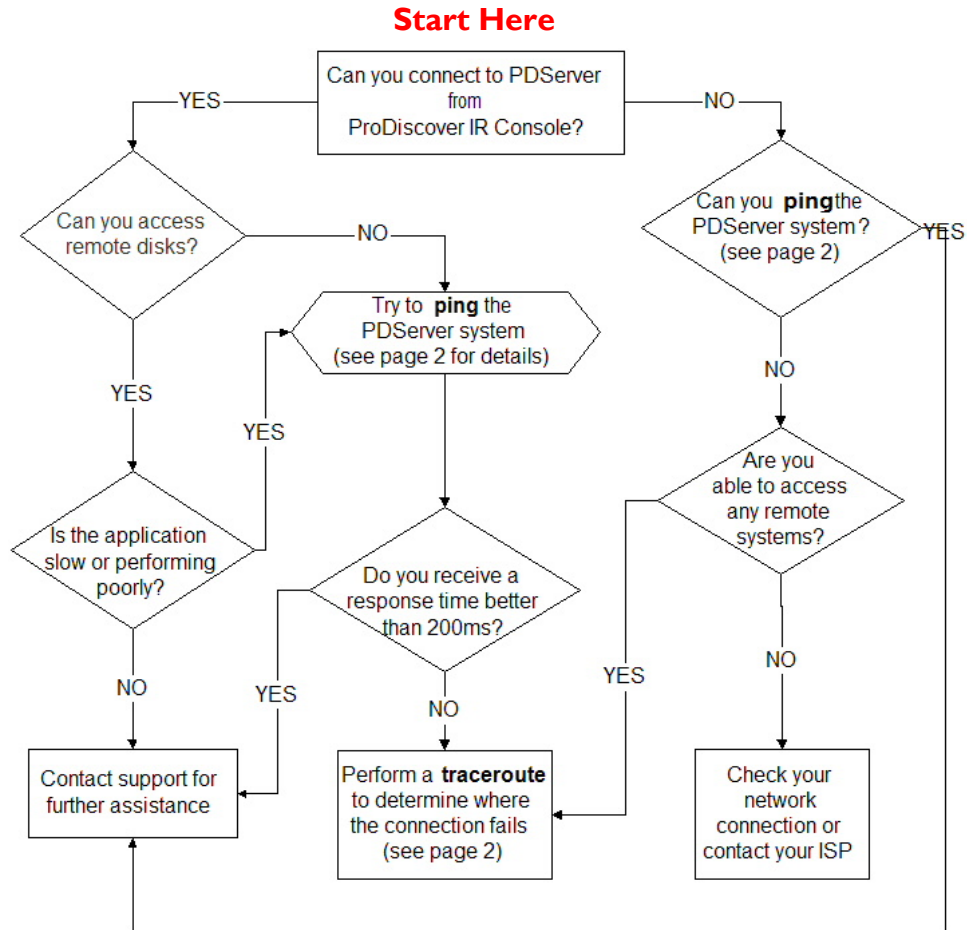
ProDiscover IR and Investigator editions offer users great power by allowing remote preview and imaging of suspect systems. Remote imaging and analysis capabilities are enabled by the use of client/server technology where the ProDiscover Console (investigators machine) is the client and the PDServer™ Remote Agent (running on the target machine) is the server. An understanding of basic TCP/IP networking is essential to successful use of ProDiscover in a network environment. Additional understanding of ProDiscover remote communications protocol can be very beneficial in streamlining connection troubleshooting. The information below is intended to provide investigators a greater understanding of ProDiscover's remote connection and basic troubleshooting techniques.

Use this diagram and accompanying information to help you determine where connection problems exist, and to provide you with the information needed to pass on to technical support to better assist you in troubleshooting problems.

You will need to know the **PDServer address** when following the chart below.

Please contact support@techpathways.com if you need help in obtaining this information.

Getting Started



Using “PING” and “TRACEROUTE” to Diagnose Problems

Ping is a simple utility that is used to check if a server is active and responding, and if it is, how long it is taking packets of information to travel from your computer to the destination server. Packets are small blocks of data (often 32 bytes of information), the sending is then checked to ensure that the data is transferred accurately. In addition to the time statistics provided, you will also receive the IP address of your destination. This can be useful in tracking domain name issues by ensuring that the domain is pointing to the correct IP address.

Traceroute is a utility that helps diagnose network congestion between your computer (ISP) and the destination server. Traceroute works by sending packets of information from your location to the destination and timing how long it takes to receive a response. In addition to tracking the time it takes to reach the final destination, you are provided with the times to each 'Hop' between your terminal and the destination. Each Hop is a separate 'router' that your information must pass through. By providing the times for each hop, we can often find the source of problems accessing a server.

Please note: While Ping and Traceroute are helpful in finding problem areas when PDServer™ is slow or unavailable, these tools do not always isolate the source of the problem. Please forward your traceroute stats to our support staff so that we can help investigate the cause of any congestion.

Using Ping in DOS (Command Prompt)

For Windows 95 and 98 users, ping is already setup to run in the DOS window, also known as the Command Prompt. To use Ping to test the connection to mcgowan.globalapp.com (your PDServer™ system), open a DOS window (*Start → Programs → Command Prompt*), and type the following command:

```
ping 192.168.0.1
```

and press [ENTER]. You should see something that looks similar to the following:

```
Pinging rtr.techpathways.com [192.168.0.1] with 32 bytes of data:
```

```
Reply from 192.168.0.1: bytes=32 time=70ms TTL=114
```

```
Reply from 192.168.0.1: bytes=32 time=70ms TTL=114
```

```
Reply from 192.168.0.1: bytes=32 time=60ms TTL=114
```

```
Reply from 192.168.0.1: bytes=32 time=60ms TTL=114
```

```
Ping statistics for 192.168.0.1:
```

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
    Minimum = 60ms, Maximum = 70ms, Average = 65ms
```

This tells you that the application server is up and running, and that the average time it took 32 bytes of data to travel from your computer to the address 192.168.0.1 and back is 65ms. Anything less than 200ms should be adequate enough for PDServer™ to function properly. However, the ideal time for the best results is less than 100ms. A connection with results in this range should provide a fast connection.

Using Traceroute in DOS (Command Prompt)

For Windows 95/98/NT/2000 users, traceroute is already setup to run in a DOS window. To use traceroute, open a DOS window (*Start → Programs → Command Prompt*), and type the following command:

```
tracert rtr.techpathways.com (your PDServer™ system)
```

and press [ENTER]. You should see something that looks similar to the following:

```
Tracing route to rtr.techpathways.com [192.168.0.1] over a maximum of 30 hops:
```

1	30 ms	40 ms	31 ms	hr1-cf9a4b01.dsl.impulse.net [207.154.75.1]
2	30 ms	30 ms	30 ms	hr4-cf9a4105.iis.impulse.net [207.154.65.5]
3	41 ms	60 ms	90 ms	q1-gateway1.impulse.net [205.171.37.69]
4	40 ms	30 ms	40 ms	bur-cntr-01.inet.qwest.net [205.171.13.169]
5	60 ms	50 ms	40 ms	bur-core-01.inet.qwest.net [205.171.13.134]
6	50 ms	71 ms	50 ms	lax-core-01.inet.qwest.net [205.171.8.41]
7	50 ms	40 ms	60 ms	lax-brdr-01.inet.qwest.net [205.171.19.38]
8	60 ms	50 ms	120 ms	4.24.118.17
9	40 ms	40 ms	40 ms	p1-0.lsanca2-br1.bbnplanet.net [4.24.5.130]
10	50 ms	70 ms	70 ms	p15-0.lsanca2-br2.bbnplanet.net [4.24.5.46]
11	40 ms	40 ms	50 ms	p7-0.lsanca1-ba2.bbnplanet.net [4.24.4.37]
12	40 ms	30 ms	41 ms	p0-0-0.lsanca1-cr4.bbnplanet.net [4.24.4.42]
13	70 ms	50 ms	60 ms	bv11.core0.sba1.netlojix.net [207.71.192.58]
14	60 ms	70 ms	70 ms	netx-rtr-e0.techpathways.com [207.71.224.129]
15	70 ms	80 ms	60 ms	192.168.0.1

```
Trace complete.
```

As you can see, it took 15 'hops' to get from the ProDiscover Console computer to PDServer™. If you experience hops with asterisks * this denotes possible congestion (packet loss) and can affect the performance of your application, or prevent you from connecting at all. When this occurs and you are having trouble accessing your server, send in a support request with the above information.

To copy this information from the Command Prompt, right-click the title bar of the Command Prompt windows, select "*Edit → Mark*", click and drag the mouse until you select the data area that you want to copy. Press [ENTER] when you've finished selecting. Switch to the Windows program that you want to import the just copied data to, and select its paste function.

ProDiscover Setup and Communications Flow

Understanding the ProDiscover Session setup and communications flow can streamline investigator troubleshooting. To provide the best possible performance in preview mode, ProDiscover's network communications is such that many small packets are sent to the target on port 6518 (by default) and many small packets are sent to the analysis console on port 6518 (by default). This approach is somewhat like the implementation of VoIP to avoid voice jitter. A simple diagram of the remote connection communications flow is seen in Figure 1.

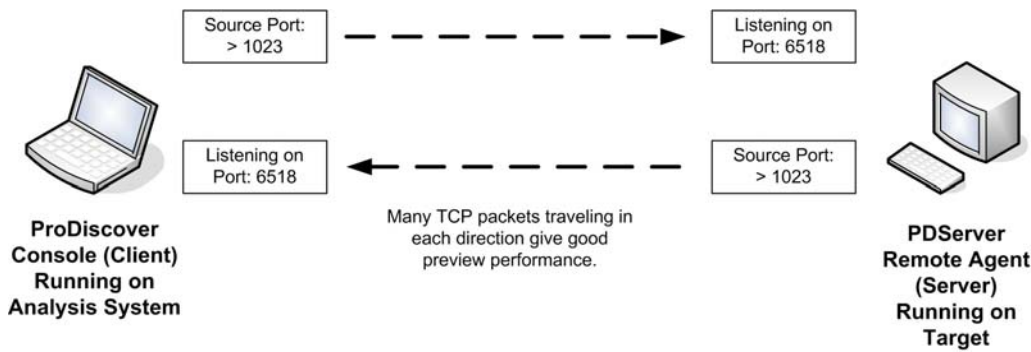


Figure 1.

Note: If the ProDiscover program is being utilized to “push” the remote agent to the target computer, then Windows File and Print Sharing ports must be open on the remote target system in addition to remote agent port 6518 (by default).

The session setup is initiated by the ProDiscover analysis console and always encrypted with 256 bit TwoFish encryption despite user settings. During session setup, packet synchronization is achieved using globally unique identifiers and any password authentication exchange is performed. The remote agent has a hard back-off algorithm to avoid brute force password attempts. To prevent packet tampering and the integrity of the one-to-one connection, any loss of packet synchronization will cause the connection to be shut down, requiring the investigator to use the ProDiscover analysis consoles network menu option for “release remote client” followed by reestablishing the connection through the connect dialog box.

Remote Push through the ProDiscover GUI

The preferred method of installing the PDServer Remote agent for many investigators is through the "Network | Install/Uninstall PDServer" menu option. Through this menu option investigators can easily set the install, uninstall, choose installation type, and remote agent settings such as the process name, port and password. If the investigator does not have the proper privileges to install the remote agent on the target machine, a dialog box will appear allowing a user name and password with the proper privileges to be entered.

Note: All installations using the "Network | Install/Uninstall PDServer" menu option are installed in Stealth mode only.

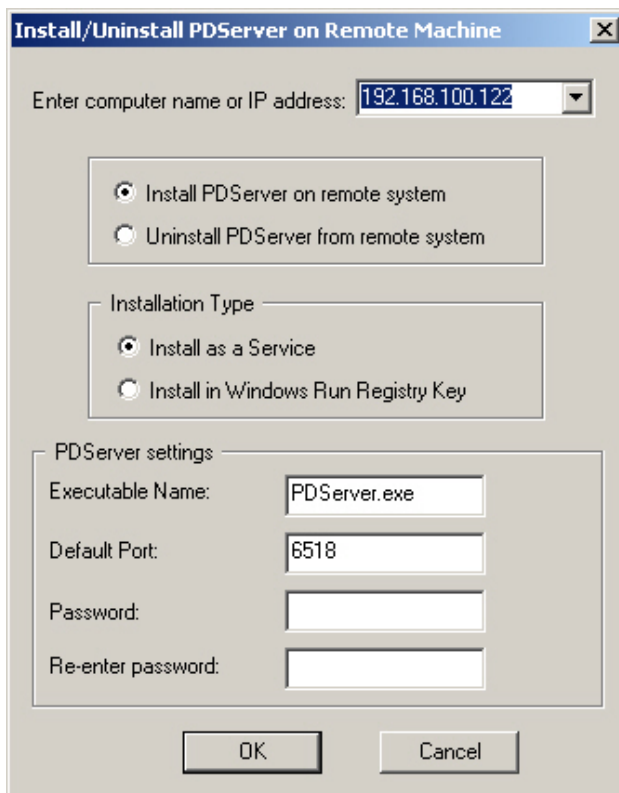


Figure 2.

Choosing to install in "Windows Run Registry Key" causes the remote agent to only run while a user is logged on to the remote system. The specific entry can be found in `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run`

Once the user presses "OK" ProDiscover will install the Remote Agent and support files in the system32 directory of the target machine. Files installed include:

- DiskI6.dll
- Disk32.dll
- msvcrt.dll
- PDServer.exe
- DFTSrv.exe (Installed only if installing as a service)
- DFTSrv.ini (Installed only if installing as a service)

Note: when choosing to rename the PDServer.exe, investigators should ensure they do not use an application name already in use by an application in the system32 directory.

If the user selects to uninstall PDServer from the remote system, all the above files will be removed with the exception of "msvcrt.dll" which may be required by other applications.

Windows XP Firewalling Guide

The Windows XP firewall, as well as other personal firewalls are by far the most common issues preventing a remote connection with ProDiscover. Understanding which ports need to be allowed on the

target system as well as the analysis console is essential. By default, TCP port 6518 should be allowed on both systems. If investigators change the default communication port on the target system from 6518, the port should be changed on the analysis console system too. i.e. The port on both systems must be the same AND be open / allowed by any firewall.

Enterprise personal firewall management tools normally allow for global firewall rule configuration changes for port allowance and application authorization. Windows XP Firewall configuration can be made in large scale enterprises using Group Policies. The Microsoft document “Deploying Windows Firewall Settings for Microsoft Windows XP with Service Pack 2” is available at <http://www.microsoft.com/downloads/details.aspx?FamilyID=4454e0e1-61fa-447a-bdcd-499f73a637d1&DisplayLang=en> or through Technology Pathways technical support contains detailed guidelines for configuration of the Windows XP Firewall in the enterprise.

In tests environments and non-domain environments the following Windows XP Firewall settings should be used.

From the Windows XP Control Panel, select the “Windows Firewall” applet. As seen in Figure 3

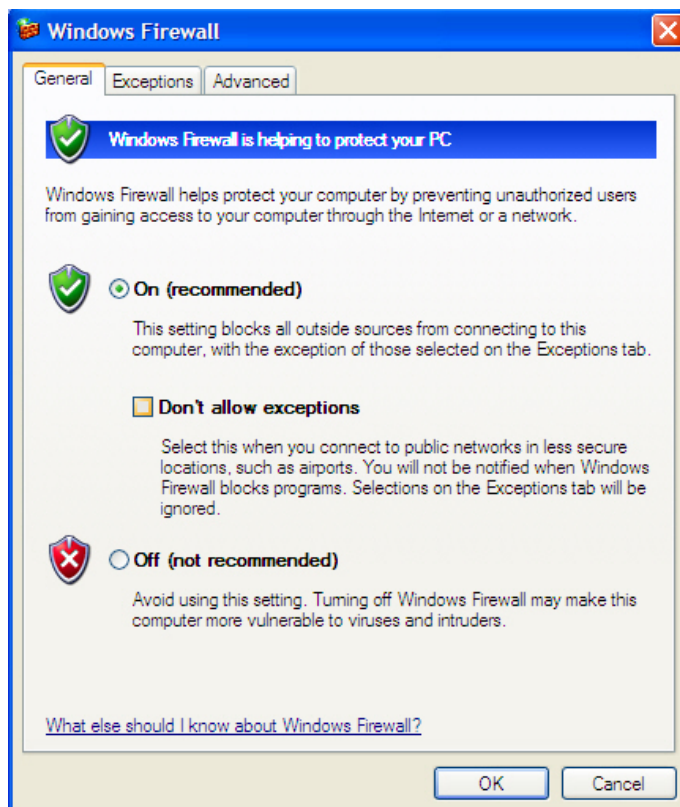


Figure 3.

Ensure the firewall is turned on and the “Don’t allow exceptions check box is not checked. It is recommended that the firewall be turned on because the Windows XP Firewall as well as other firewalling products are known to filter traffic even when turned off.

Choose the “Exceptions” tab.

Note in Figure 4 the entry for “DFT” This is a program entry that is automatically created on the analysis console system if the user chooses to allow ProDiscover when first run and the Windows XP Firewall

attempts to block it from binding to the default port of 6518.

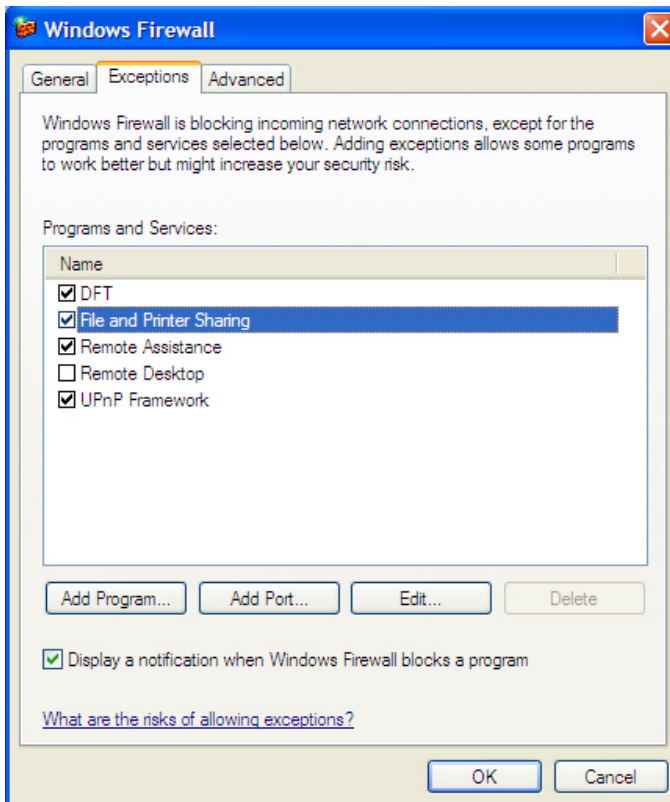


Figure 4

Ensure that the “File and Printer Sharing” Dialog box is enabled to allow the ProDiscover Remote Agent to be “Pushed” out from the ProDiscover console network menu option.

If this is the target system and ProDiscover had not been installed the “DFT” option will not be present and is not required.

The “Add Port...” button is used to allow TCP and UDP ports to pass. The default port of 6518 or other desired ports should be added on any remote system with the Windows XP Firewall intended to be a target system as seen in Figures 5 and 6.

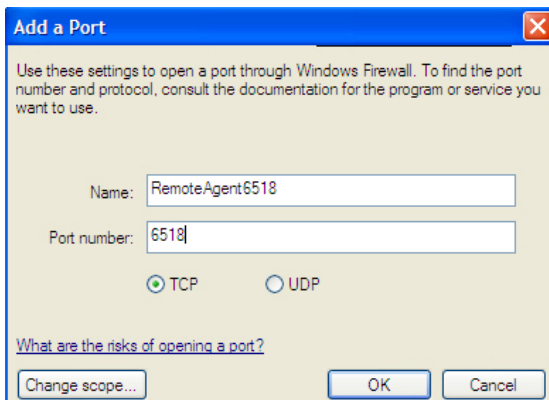


Figure 5.

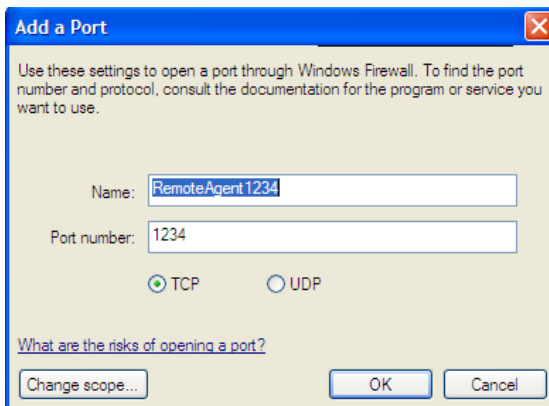


Figure 6.

Once the ports have been added they can be enabled and disabled from the “Exceptions” tab as seen in Figure 7. Note: These port additions should also be made on the analysis console system.

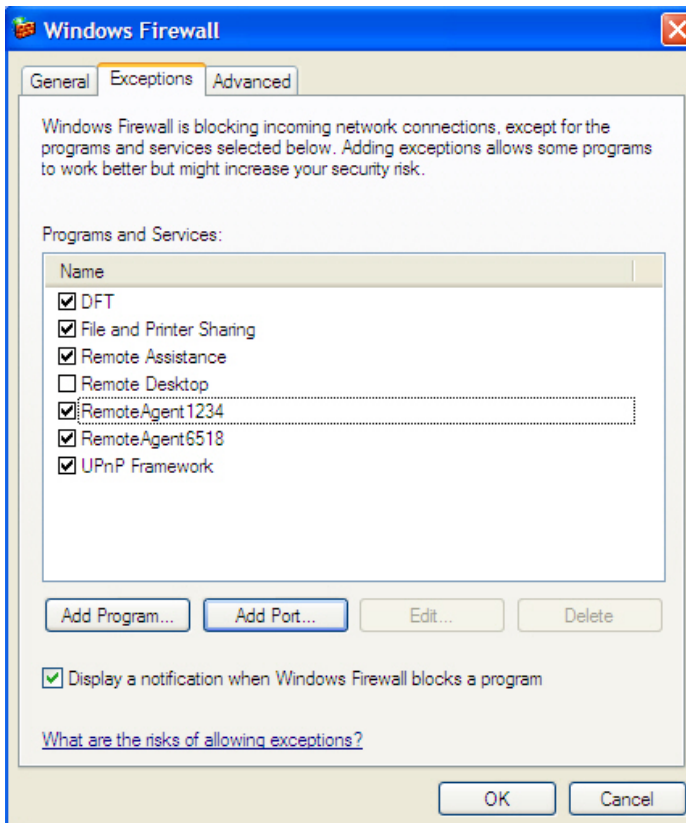


Figure 7.

The “Advanced” Tab as seen in Figure 8 allows users to enable firewall logging through the “Security Settings | Settings” button. Firewall logging can be very helpful in troubleshooting failed connections.

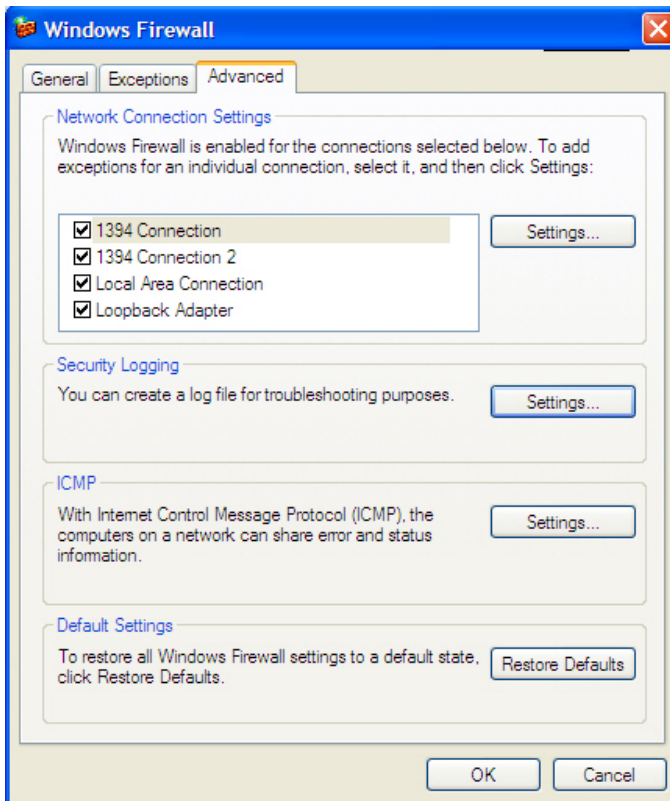


Figure 8.

Many systems today use personal firewalls such as the Windows XP Firewall added in Service Pack 2. Most can also be configured as described above. The key is that the ports being utilized (6518 by default) should be allowed on both systems. Windows File and Print Sharing should also be allowed on any target system that investigators desire to “push” the PDServer Remote Agent to.

Windows 2000 Packet Filtering

Administrators who are very security minded will often use the simple packet filtering available in Windows 2000 to add an additional layer of protection. This is particularly true on internet facing host and other high-risk servers. Packet filtering is an important component of any firewalling approach and as seen in the Windows XP Firewall, is important to configure properly.

If investigators are having difficulties connecting to a target Windows 2000 server even after checking any personal firewalls it is helpful to check for Network Adapter Packet Filtering using the following steps.

From the Control Panel “Network and Dial-up Connections” applet, highlight the “Local Area Connection” in question, right-click and choose “Properties”. A dialog box as seen in Figure 9 will appear.

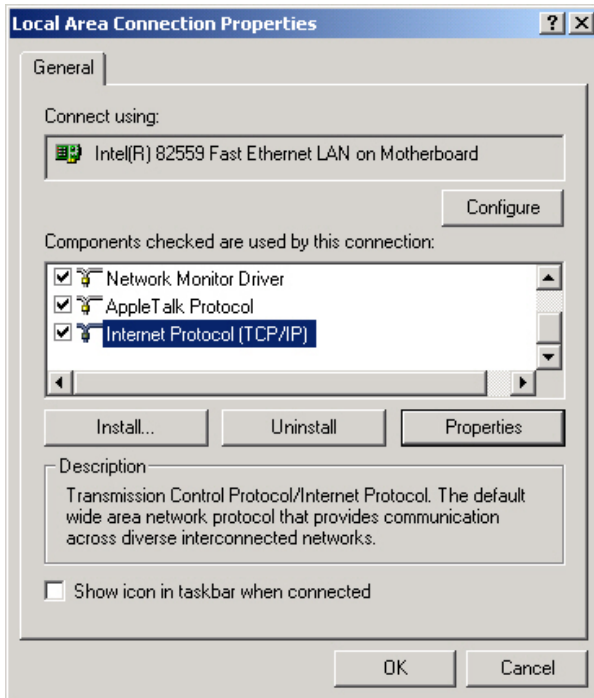


Figure 9.

From the “Local Area Connection Properties” dialog box, highlight the “Internet Protocol (TCP/IP)” component and choose the “Properties” button.

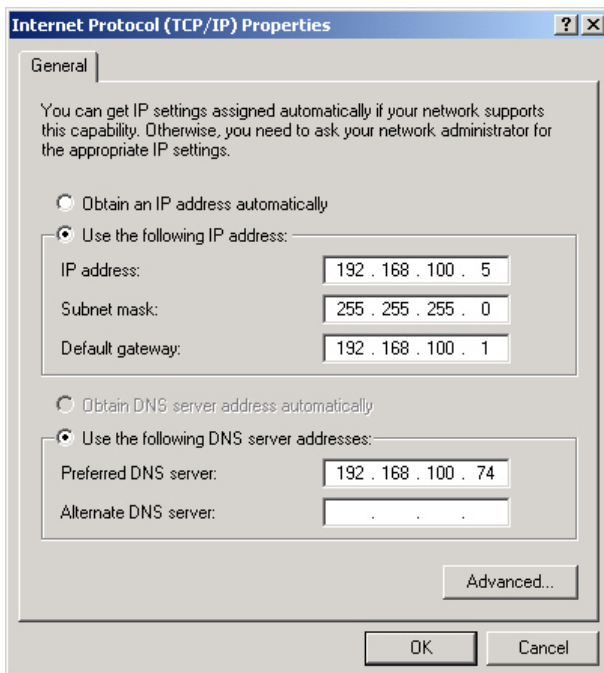


Figure 10.

In the “Internet Protocol “TCP/IP) Properties” dialog box that appears as shown in Figure 10 choose the “Advanced...” button. The “Advanced TCP/IP Settings” dialog box will appear as shown in Figure 11.

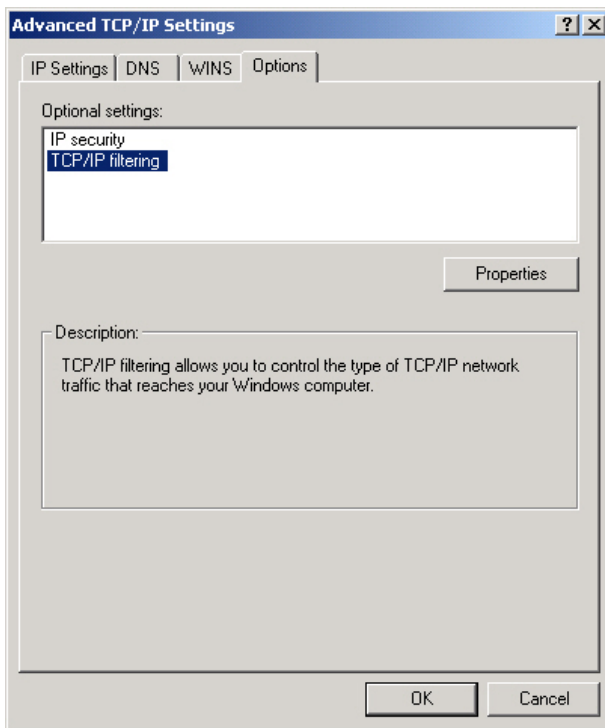


Figure 11.

From the “Advanced TCP/IP Settings” dialog box highlight “TCP/IP filtering” and choose the “Properties” button to bring up the TCP/IP packet filtering dialog box as seen in Figure 12.

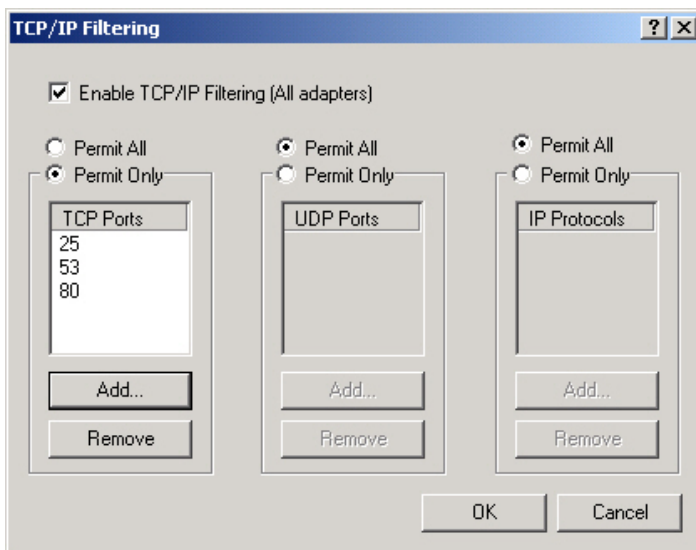


Figure 12.

If the “Enable TCP/IP Filtering” check box is enabled and the “Permit Only” radio button for TCP Ports is selected, investigators have the option of disabling the “TCP/IP Filtering” check box or adding the PDServer Remote Agent port to TCP Ports. Note after the change is made and the investigator chooses OK, a system reboot is required for the changes to take effect.

This type of packet filtering is only normally found on Internet facing and high-risk servers however, it is often overlooked and can be difficult to troubleshoot.

Troubleshooting Timeouts & Performance

Obsessive timeouts during protracted functions such as imaging, or more in-depth analysis can be caused by many things. Some troubleshooting and planning can often limit these difficulties.

One of the first things to look at is the end-to-end network utilization and performance between the analysis console and the target system. The better the performance the less likely timeouts will occur. Because of the amount of data being transferred, good network performance is critical.

The next consideration is related to ProDiscover's design. We are designed to provide minimal impact on the target system so as to allow background monitoring. All ProDiscover Remote Agent processes run at a low thread priority. If the target system becomes busy for protracted periods of time, this could preempt our process and thus cause excessive timeouts. Investigators can increase the PDServer.exe thread priority on the remote system to overcome this effect if desired. Process thread priority can be changed through the Windows Task Manager's Process tab by highlighting the desired process, right-clicking and choosing "Set Priority".

Another consideration is also related to ProDiscover's design. To provide the best possible performance in preview mode, ProDiscover's network communications is such that many small packets are sent to the target on port (6518 by default) and many small packets are sent to the analysis console on port (6518 by default). Somewhat like VoIP does to avoid voice jitter. This design can overload the TCP/IP buffers on the console and/or target systems. To prevent timeout issues along these lines we make some TCP/IP stack performance enhancements on the registry of the analysis console machine during ProDiscover installation. In some cases making these registry changes on the target system can eliminate any timeout issues. The default installation directory of ProDiscover contains a .reg file called "ProDiscoverRegistryTweak_2k_XP.reg" that will make these changes to any Windows 2000, 2003, or XP system. Note a system reboot is required after making these adjustments and system performance is increased by making the change.

In summary, ProDiscover performance is directly affected by the performance of the systems and network that it is being used in, more so than many applications due to the volumes of data that may be accessed. That said, Technology Pathways is continually researching ways to increase performance and improve the application through the utilization of user feedback.

Push Checklist

If the push fails to authenticate with the remote system, are you providing account credentials with local administrative rights on the target system?

If the answer to #1 above is yes, but the authentication still fails, then check the default Windows XP (non domain environment) settings on the target system. Ensure that the security options policy for "Network access: Sharing and security model for local accounts" is set for "Classic – local users authenticate as themselves" (The default setting is "Guest only – local users authenticate as Guest"). This is documented in detail on the ProDiscover Community forums at <http://toorcon.techpathways.com/CS/forums/98/ShowPost.aspx>

If the answer to #1 is still yes, but authentication fails, check to ensure the administrator account is enabled on the target system and ensure that the security options policy for "Accounts: Limit local account use of blank passwords to console logon only" is set for "Disabled" (The default setting is "Enabled"). These settings are normally only required on non-domain (workgroup) computers. This is documented in detail on the ProDiscover Community forums at

<http://toorcon.techpathways.com/CS/forums/99/ShowPost.aspx>

If attempts to “Push” the agent timeout and fail with no authentication request from the remote system, check the Windows XP Firewall settings and ensure that “File and Print Sharing” is allowed under “Exceptions”. Note this setting is only present in non-domain (workgroup) installations.

Connection Checklist

Can you ping the target system? Remember that Ping blocking could be on the client, server, or the network and failure does not definitively indicate a problem.

If you changed ports on the remote agent, did you change the User preferences on the ProDiscover Console to match?

Does the remote system have a firewall? If so, is it set to allow the ProDiscover/PDServer port through (6518 by default)?

Does the local system have a firewall? If so, is it set to allow the ProDiscover/PDServer port through (6518 by default)?

If Windows XP Firewall is installed it is recommended to be turned ON at both analysis console and remote target systems with exceptions made for the ProDiscover Port in use (6518 by default). Note Windows XP and other personal firewalls have been known to enforce port blocking when turned OFF.

Is there a hardware firewall or are access lists being enforced on a switch in-between the analysis console and target system? If so the port in use (6518 by default) should be allowed in both directions.

Introduction to the ProScript API and Perl

Various editions of ProDiscover (All current editions excluding ProDiscover for Windows) support ProScript, a scripting language to perform user-defined tasks on the disk or image within the current Project. In order to achieve this task, ProDiscover supports an API to be used by a ProScript programmer in conjunction with the embedded ActiveState ActivePerl engine. The ProScript programmer calls these functions as if they are native functions within Perl.

Writing and Debugging ProScripts

Programming in Perl using the ProScript APIs provides a great deal of power to the investigator. With this power comes the power to crash ProDiscover or damage local files when using the Perl APIs. Investigators should have a complete understanding of any scripts they are working with prior to use in live cases.

WARNING: While ProScript will not write to evidence disk or images in any way, BE ALERT: the use of Perl File IO to open an image file can damage the image. ALWAYS: Users should ensure all image read functions are performed from ProScript API's. ALWAYS: Users should understand and test all scripts prior to use on actual evidence images. REMEMBER: Hardware write blockers can help to protect image files from external applications."

One of the most difficult issues when programming in any language is identifying syntax errors. Simple mistakes such as typing "PSCloseHandel(\$nHandle);" when you meant to type "PSCloseHandle(\$nHandle);" or simply missing an ending ";" can be difficult to track down. Two techniques to help identify and overcome syntax errors are:

Use a graphical user interface programmers editor capable of highlighting syntax errors and keywords. There are many such editors available. Technology Pathways recommends PrimalScript from SAPIEN (www.sapien.com) and Komodo from ActiveState (www.activestate.com). Both are fine editors suitable for Perl programming. The PrimalScript editor allows users to create a Perl.ext file to add ProScript APIs to Perl's keywords for proper highlighting.

While ProScripts must be run from ProDiscover, executing a ProScript from the command line during development can be useful in identifying syntax errors such as missing statements or braces.

Note: Before attempting to run ProScripts the user should choose "Install Perl Module" from the "ProDiscover" start menu item. The Install Perl Menu item is a batch file that will copy all necessary files from the ProDiscover installation directories to the Perl default directories.

Once the ProScript Modules are installed properly writing ProScripts is as simple as adding:

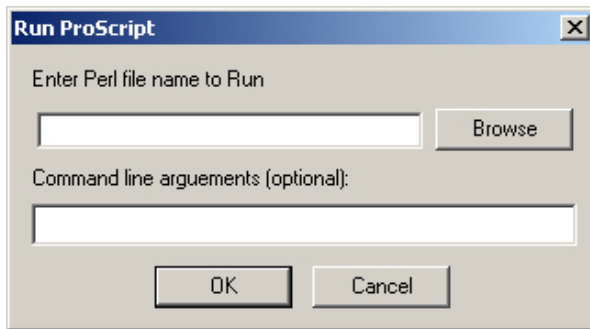
use ProScript;

to standard Perl code.

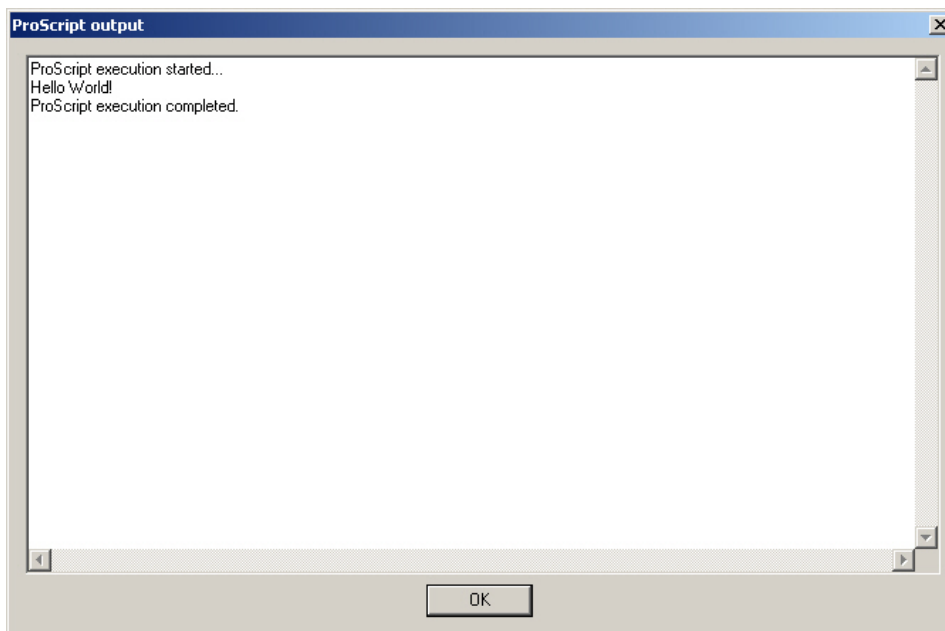
The simplest Hello World programming example using ProScript in Perl is to create the file helloworld.pl with the following contents:

```
use ProScript;  
PSDisplayText("Hello World!");
```

When run from the ProScript input dialog box:



Will produce the following output:

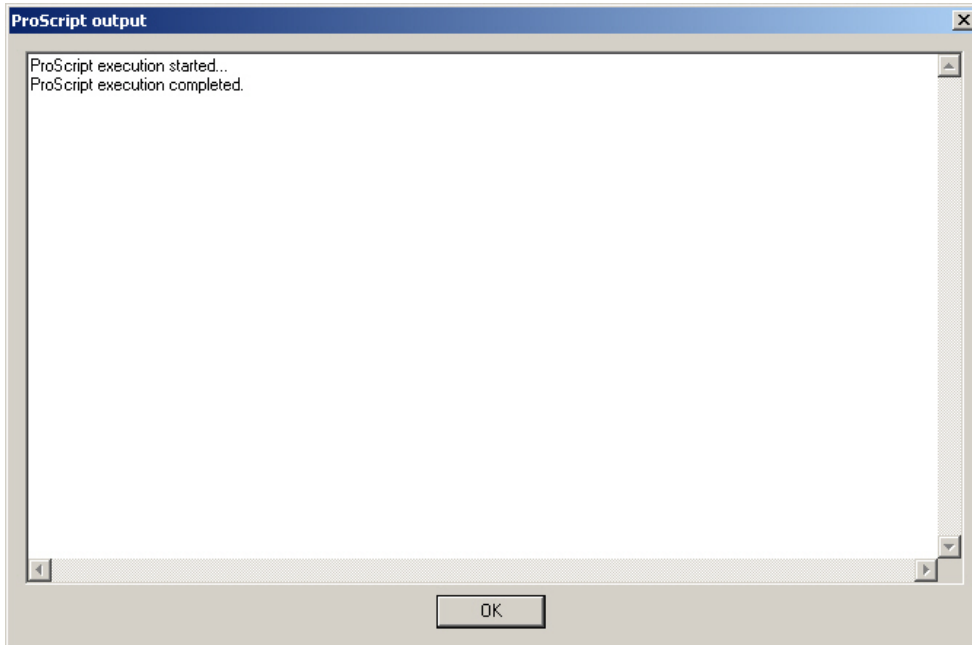


Investigators should note that Perl and ProScript are case sensitive. By simply changing the lower case "u" in use to "U" as in:

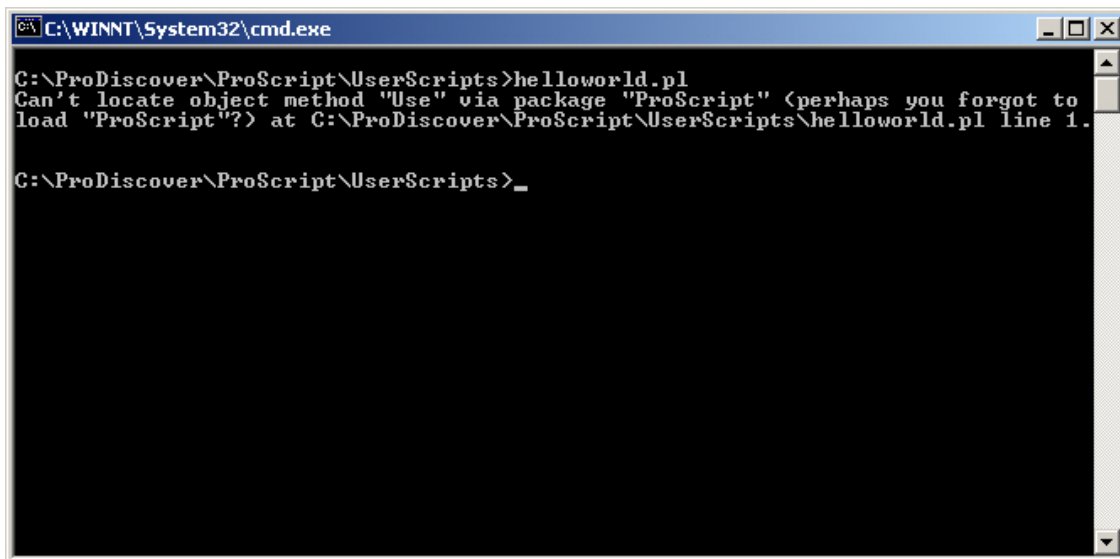
```
Use ProScript;
```

PSDisplayText("Hello World!");

The output results become unexpected as seen in here:

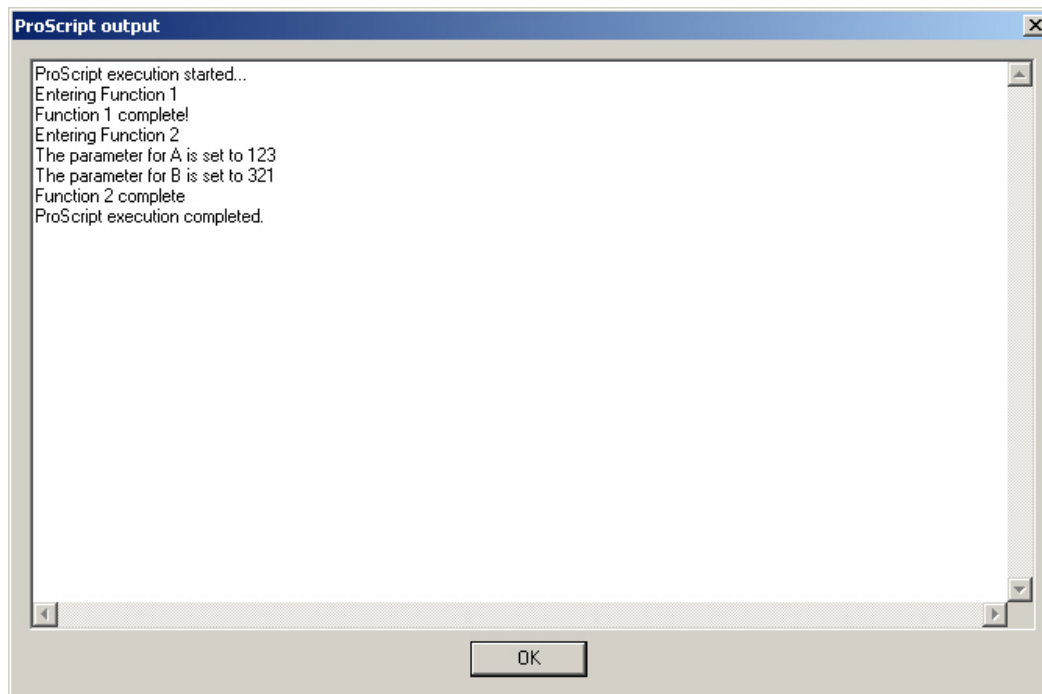


By using the tip from above to check our scripts syntax by running from the command line investigators can quickly identify the offending statement in the code above.



Once syntax errors are overcome, debugging logic flow and veritable initialization issues can be tracked

down by heavy use of `PSDisplayText()`; statements. By placing `PSDisplayText()`; statements throughout ProScripts during the debugging process, and investigator can follow the flow of their statement execution in the ProScript output window as seen below:



As seen above displaying a scripts execution status to the ProScript output window can be useful in identifying logic and parameter initialization issues.

Debugging scripts during development can become frustrating, but the pay off can be tremendous. Once scripts are completed a well written script will require very little modification and can greatly automate the investigative process. Technology pathways provides an online forum for the exchange of ProScript ideas and posting of user scripts. The forum can be located at the following URL <http://toorcon.techpathways.com/CS/> or through the Support section of the Technology Pathways Web site at www.techpathways.com.

For details and examples of each ProScript function please refer to the ProDiscover ProScript Manual. Documentation, program and example files are also installed in the ProScript directory found within the program installation directory as follows:

\ProScript\Documentation - contains ProScript API documentation.

\ProScript\Examples - contains ProScript API and Perl example scripts.

\ProScript\PerlModules - contains ProScript Perl module setup files and installation batch file.

\ProScript\User Scripts – contains more complete working ProScripts

Advanced tips and tricks



Deleted Files.

Each Windows disk contains a hidden folder named Recycled (FAT/FAT32), or Recycler (NTFS). This folder is where Windows 9x and Windows NT/2000 keeps deleted files.

When a user deletes a file, the complete path, file name and date of deletion is stored in a hidden file called INFO or INFO2 (Windows 98/2000) in the Recycled/Recycler folder. The deleted file is renamed, using the following syntax:

D<original drive letter of file><#>.<original extension>

Example:

New file name:

Dc1.txt = (C drive, second file deleted, a .txt file)

INFO file path:

C:\Windows\Desktop\Cards.txt

Each Windows drive will contain a Recycled/Recycler folder upon the first file deletion.

Note: ProDiscover will parse the INFO/INFO2 File and interpret the results if desired. Just right click on any INFO or INFO2 file from Content View and choose "View as INFO".



ATA Hardware Protected Areas (HPA).

ATA Specifications added the "Protected Area" as a means for PC distributors to ship diagnostic utilities with PCs. Simply put, the hardware protected area is an area of the hard drive that is not reported to the system BIOS and operating system. Because the protected area is not normally seen, most disk forensics imaging tools will not image this area. We have seen an emergence of new utilities available allowing PC users to take advantage of this "Protected Area" to store user data. One such utility is the commercial product AREA51.

In some cases forensics examiners can identify the use of the Protected Area by analyzing the boot partition which may contain boot options for the area. Current versions of AREA51 modify the boot partition by changing the boot loader to include pointers to the protected area.

Users can also detect the Use of an ATA Protected Area by doing a little disk math. Consider the following scenario:

The user is about to image a disk which is labeled or they know has a CHS (Cylinder Head Sector) value of 16383/16/63. In this case to find out the total number of sectors which should be reported simply multiply (Cylinders x Heads x Sectors). In this case $16383 \times 16 \times 63 = 16,514,064$ total sectors. If the user started an image of the disk and noticed it only reported 4,192,965 sectors then they would be missing around 6 gigs of data area depending on how many bytes were used in each sector. To establish the total disk size use total sectors x bytes (normally 512). In this case the disk should be 8.4 GB, but was reporting about 2 GB.

ProDiscover includes a device driver that allows ProDiscover to detect and look inside the Hardware Protected Area. When ProDiscover is launched the device driver reads all Hardware Protected Area information from the disk to detect if the HPA is in use then sends a single command, "SET MAX ADDRESS" (Volatile option) to any disk added to the project. This process allows users to image the complete drive. In accordance with the HPA technical specifications, once the machine is power-cycled the drive is automatically returned to its original state.

Often ProDiscover will automatically detect and add file system partitions within the HPA to your directly added disks so they may be viewed as a normal partition in Content-View or Cluster-View. Since the HPA technical specification does not specify where a file system starts or what type of file system resides within the HPA, ProDiscover provides a tool for scanning the HPA to detect any file systems inside and adding the file system partition to the current project. All file systems added to a project from the HPA will have [HPA] appended in the tree-view to clearly identify their origin. See Using ProDiscover for specific steps and tasks involving the HPA.

Technology Pathways also provides a DOS utility application "PAREmove.exe" that allows forensics examiners to remove the Hardware Protected Area permanently thereby enabling any other imaging tool to image all sectors of the disk. If the examiner suspects that the Hardware Protected Area has been utilized on the disk, they only need run PAREmove.exe from a DOS boot disk to remove the HPA.



Alternate Data Streams in Windows NT/2000/XP.

Alternate Data Streams (ADS) have been available to Windows NT and 2000 systems ever since the first version of NTFS. ADS was originally created to allow Windows NT to support Macintosh computers which keeps some file information in Resource Forks.

While ADS was created for Mac file support, any user can utilize ADS to hide data or files within a system which uses NTFS formatted drives. It is easy to hide data with ADS and only requires a few steps as shown by the following:

1. From command line in Windows NT/2000 Pro enter C: to move to drive root
2. Enter "notepad boot.ini:ADSFile.txt"
3. Notepad asks to create the file, choose OK
4. Type in some text to hide
5. Choose file | save
6. Exit notepad
7. Enter "notepad boot.ini:ADSFile.txt"
8. Confirm the text you entered is still there

Now try the same thing without appending the ADS to any file.

1. From command line in Windows NT/2000 Pro enter C: to move to drive root
2. Enter "notepad :AnotherADSFile.txt"
3. Notepad ask to create the file choose OK
4. Type in some text to hide
5. Choose file | save
6. Exit notepad
7. Enter "notepad :AnotherADSFile.txt"
8. Confirm the text you entered is still there

While ADS files are not viewable in Windows NT/2000 through normal file views, there are several utilities which allow you to detect the presence of ADS files. Unfortunately these utilities do not always detect the presence of all ADS files. In particular ADS files which have not been created as appended to a visible file are sometimes not reported. ProDiscover detects and displays all ADS files and displays them in "**Content View**" highlighted in **Red** by default.



System \$ meta files in Windows NT/2000/XP.

When viewing an NTFS partition in Content-view users will notice files not normally seen which all begin with \$ and are highlighted in **green** by default. These files are NTFS meta files and contain a great deal of information about the file system.

Each metafile has an inode number and description as listed here:

- Inode 0 \$MFT Master File Table - An index of every file
- Inode 1 \$MFTMirr A backup copy of the first 4 records of the MFT
- Inode 2 \$LogFile Transactional logging file
- Inode 3 \$Volume Serial number, creation time, dirty flag
- Inode 4 \$AttrDef Attribute definitions
- Inode 5 . (dot) Root directory of the disk
- Inode 6 \$Bitmap Contains volume's cluster map (in-use vs. free)
- Inode 7 \$Boot Boot record of the volume
- Inode 8 \$BadClus Lists bad clusters on the volume

Inode 9 \$Quota NT Quota information

Inode 9 \$Secure 2K Security descriptors used by the volume

Inode 10 \$UpCase Table of uppercase characters used for collating

Inode 11 \$Extend 2K A directory: \$ObjId, \$Quota, \$Reparse, \$UsnJrnl

A great deal of information about these files and the NTFS file system can be found online at <http://linux-ntfs.sourceforge.net/ntfs/index.html>



EXIF Meta Data found in JPG and TIFF graphics files.

The Japanese Electronic Industry Development Association (JEIDA) created a standard for the storage of camera and image metadata in JPEG and TIFF files. Most digital camera manufacturers have implemented this standard and now store camera metadata along with the digital image. This metadata can potentially provide vital evidence to investigators such as when the picture was taken, what camera was used in capturing the image and in some cases, who took the image or where the image was captured.

The Tag tables in EXIF meta data provide a tremendous amount of potentially useful information if contained in the EXIF section of a JPEG file. While it is cumbersome to try to pull this data manually from the file, programs exist today to extract this data for the investigator. Programs such as EXIFutils or IMatch can be used to view this information. Technology Pathways forensic tool, ProDiscover will automatically extract and report this information for investigators if desired for all JPEG and TIFF files marked as evidence of interest. This can open up a whole new avenue for investigators and capture EXIF metadata in an evidentiary quality manner to be used in court at a latter date.

To view the EXIF meta data of a JPG or TIF file in ProDiscover simply right-click on any .jpg or .tif graphic file from content-view and select "View EXIF data"



Timeline Analysis Techniques.

Common timeline analysis techniques often focus on the Modified, Accessed, and Created, or MAC timestamps placed on files in the NTFS file system. Some investigations benefit by understanding how normal MAC times relate to lower level information such as when specific metadata attributes were changed.

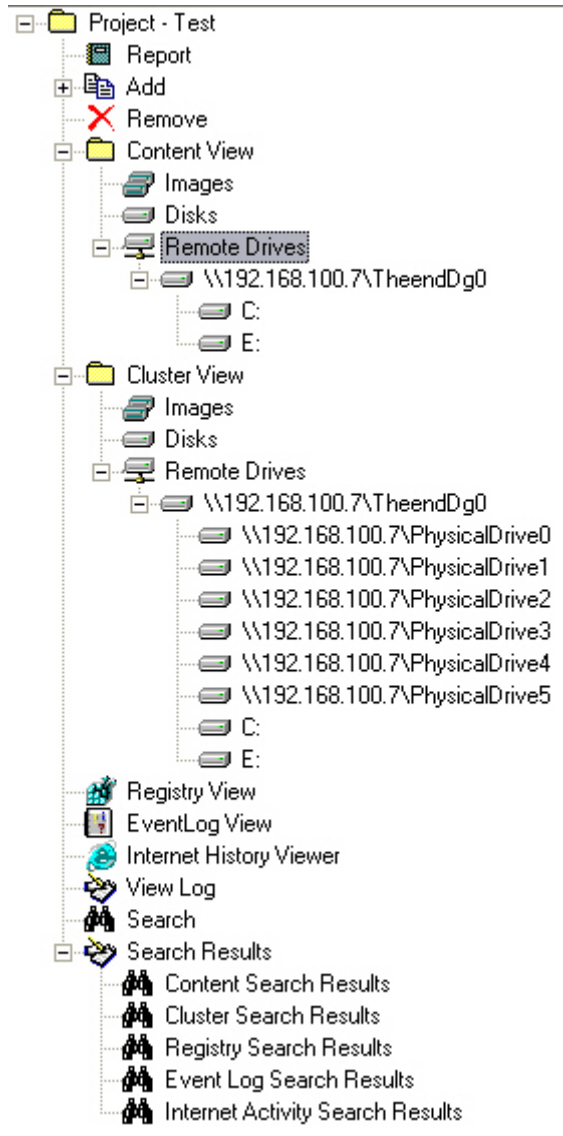
Two metadata attributes of interest to investigators in the NTFS file system are the Master File Table (MFT) \$STANDARD_INFO and \$FILE_NAME. Both attributes contain their own entry last modified timestamps that are displayed by ProDiscover in the project report and in sortable columns in the content view work area. The MFT \$STANDARD_INFO attribute contains general information about a file such as flags, last accessed, written, created times, owner, and security ID. The MFT \$FILE_NAME attribute contains file name in Unicode, and also the last accessed, written and created times. MFT entry modified times can be found in the project report as "MFT STANDARD INFO entry modified:" and "MFT FILE NAME entry modified:" These values are listed in the content-view work area in columns as "MFT \$STANDARD_INFO Modified" and "MFT \$FILE_NAME Modified".

(This page intentionally left blank.)

Appendix A: ProDiscover Commands

Tree View Commands

When a project is opened the user will be presented with a tree-view of selections under the project name as shown below.



Functions available within the tree view are:

Report

This item in the tree-view and view menu will be enabled only when a project is opened. Selection of this item from the tree-view will display the default project report in the work area with the following headings:

- Evidence Report for Project:
- Project Number:
- Project Description:
- Image Files:
- Disks:
- Evidence of Interest:
- File Signature Mismatch:
- Search Results:
- Project Notes:

Each report heading will be automatically populated during the project session with resulting data from user actions. Enabling a file or directory's "selected tag" within Content View will atomically add that file or directory to the "Evidence of interest" heading within the report. The "Project Notes" heading is a place holder for user notes to be added once the user has exported the report for editing in their favorite word processor.

While working a project, users may find it necessary to clear data within report headings such as, "Evidence of interest" and "Search Results". Removal of data within these headings is easily accomplished using the action menu's "Clear Report - Evidence of Interest and Search Results" function. Removing a disk or image file will atomically remove that items associated information from the report.

Add | Capture & Add Image

Selection of this item from the tree-view, or action menu captures and adds an image to the current project. When capturing the image, this function creates a bit stream image of the drive selected, based on inputs provided by the user, to password protect and compress the file. It saves the file as an Image file at the destination provided by the user. After an image is captured and written to a file, a hash will be computed allowing the user to verify image integrity.

Add | Image

Selection of this item from the tree-view, or Action Menu will display a file open dialog for selection of an Image file to be added to the current project. The file dialog will look for image files with extension ".eve", ".pds" or ".pdg". *.eve is the default ProDiscover image format.

If the image is of a Windows NTFS Dynamic Disk, users should select the image's corresponding *.pdg file which describes the disk group. If the image was a ProDiscover Split image, users should select the *.pds file which describes all split files comprise the total disk image.

UNIX style "dd" images can be added to projects provided with or without the .eve file extension. To add a dd image to the project without an expected extension choose "All Files (*.*)" from the "File of Types" Drop down list. If the "dd" image is split into several images they should be numbered sequentially and all contain a .eve file extension. Once the image files are named and numbered correctly a corresponding *.pds file should be created in the following format:

```
DD-SplitImage
Split0.eve
Split1.eve
Split2.eve
Split3.eve
Split4.eve
```

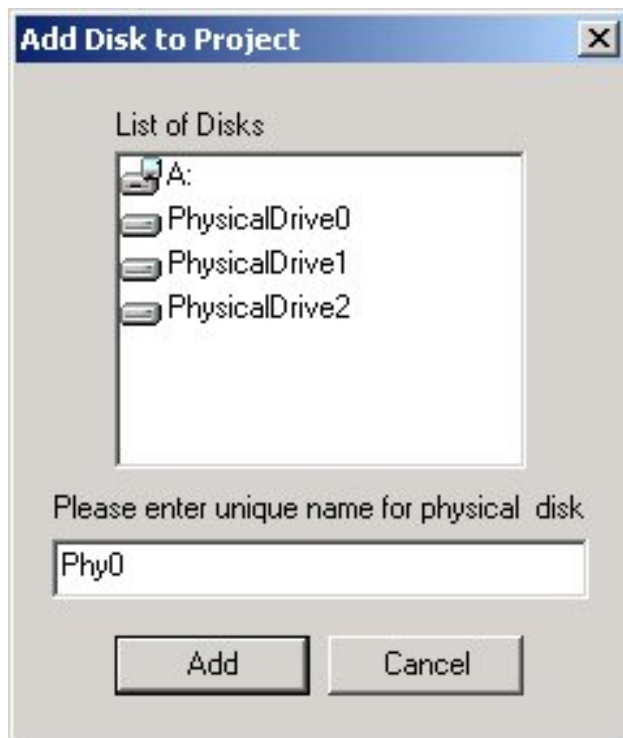
Note that all split image file should be split in sizes which are multiples of 512. To add the split "dd" image

users should select the split.pds file created above.

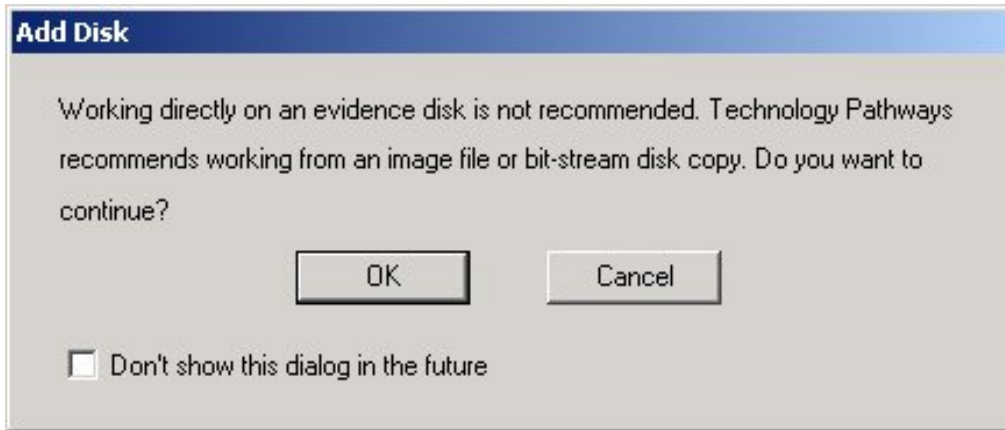
Add | Disk

Selection of this item from the tree-view, or action menu will allow the user to select a hard disk or Disk Group from the local system or system connected through PDServer™ Remote Agent and add it to the project.

Note: Disk Groups are a single disk or group of dynamic disks in Windows NTFS formatted systems. Dynamic disks are physical disks that don't use partitions or logical drives. Instead, they contain only user created dynamic volumes. Dynamic Disks are used to create fault-tolerant volumes such as striped, mirrored, and RAID-5 volumes. Dynamic Disks can also extend volumes and make changes to the disk without rebooting the computer. ProDiscover supports previewing and imaging Dynamic Disks.



Once selecting "Add" you will receive the following warning:



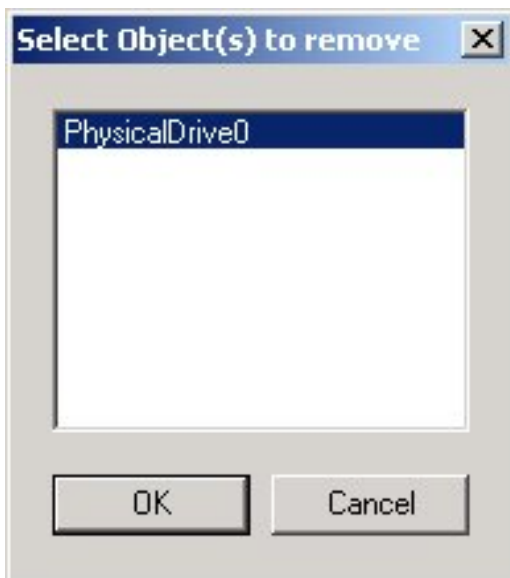
Users can safely disregard this warning if the disk they are adding to the project is a bit-stream image of original evidence and you have installed the image to a system bus with write-blocking capabilities. **Note:** while ProDiscover will not write to any image or drive the operating system will without hardware write-blocking.

It is recommended to use a hardware write-blocking device for analyzing directly attached bit-stream evidence copies. Several such cards widely available are:

- NoWrite™ IDE write blocker (allows ProDiscover access to the Hardware Protected Area "HPA") <http://www.techpathways.com>
- ACARD SCSI-to-IDE Write Blocking Bridge (AEC7720WP) <http://www.microlandusa.com/>
- Intelligent Computer Solutions, Inc. <http://www.ics-iq.com/>

Remove

Allows the user to remove image file or disk associations with the current project. This action does not delete any files or disk.



Content View | Image

1. This item in the tree-view and view menu will be enabled only when a project/image file is selected.
2. Selection of this item from the tree-view or view menu will display the contents of the Image file in the work area. The data files and the folders contained in the disk image captured will be displayed in the work area in a tabular form with information such as: selected tag, file name, file extension, size, modified, accessed and created times, as well as, file attributes. File attribute codes are as follows:
 - **r** = Read-only file
 - **a** = Archive file
 - **s** = System file
 - **h** = Hidden file
 - **d** = Folder
 - **ADS** = Alternate Data Stream File
 - **k** = any file that matches a Hashkeeper compare operation
 - **m** = any file that contains a signature mismatch after a signature mismatch evaluation if run.
3. When enabled, the "selected tag" causes ProDiscover to create a cryptographic checksum of the item and insert it into the "Evidence of Interest" section of the project report. Cryptographic checksums are created in the algorithm set by the user in the preferences setting. MD5 is the default algorithm used for checksums. Depending on the processor power available, enabling the "selected tag" can take a few seconds per file due to the checksum creation.
4. The list shall also include the files marked as deleted by the OS.
5. Double-click on any file (e.g. file.txt) will display the contents of that file with the default viewer for that type. It is assumed that the default viewer for the file type is available on the machine. If there is no such viewer, a choose application dialog box will be displayed allowing the user to choose an application to view the file with.
6. Right click on a single file allows the file to be recovered and copied to a destination of choice, including files marked as deleted.

Notes: The "Deleted" column will display "Yes" if the file has been deleted. On NTFS formatted drives, ProDiscover collects all deleted files into a special directory called "Deleted Files" which is not normally present on the original drive. The "Deleted Files" directory is a virtual directory for ProDiscover to recover deleted files in cases where a deleted file can be recovered, but the original path can not be found.

Content View | Disk

1. This item in the tree-view and view menu will be enabled only when a project/disk is selected.
2. Selection of this item from the tree-view will be similar to view image file, except that it will display the contents of a directly attached disk which has been added to the current project.

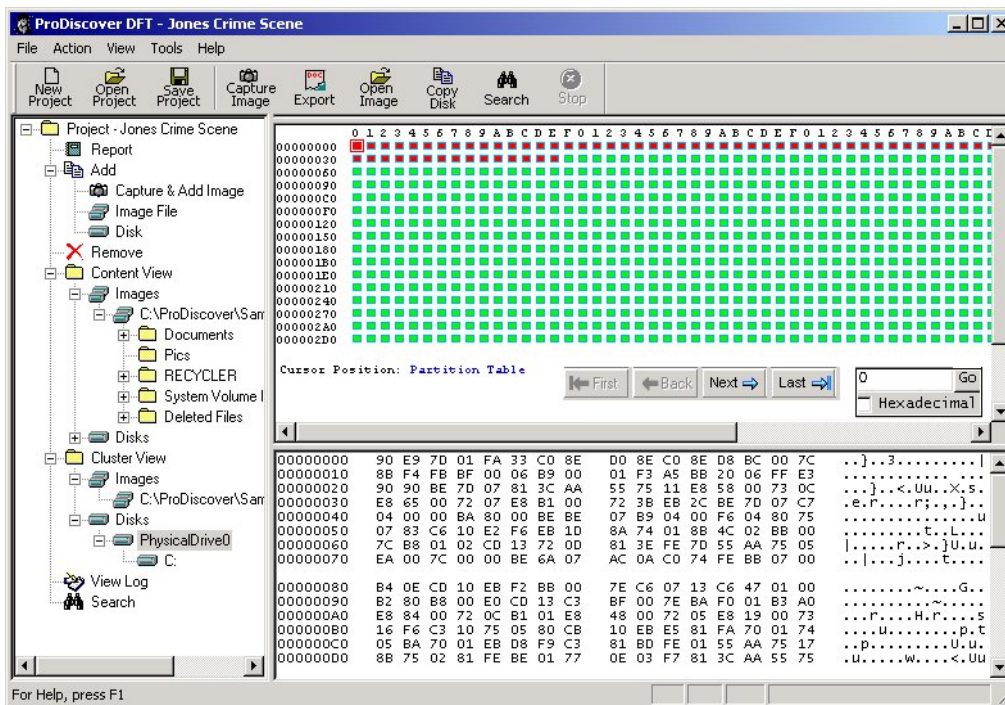
Cluster View

1. Selection of this item from the tree-view items will display the directly connected disk or an image file as a grid of clusters in the work area with the contents of the cluster in the display area below.
2. The Zero cluster displays all boot sector and partition data and all subsequent clusters contain actual file system data which are marked "used", or "unused".
3. The user can easily navigate through the clusters using the navigation buttons below the cluster

- grid and with left and right mouse clicks.
4. Selecting an individual cluster will display its contents in the display area in ASCII text and Hex format.
5. With the physical drive selected from the tree-view the user can view all boot sector and unallocated disk space, as well as all partitions and file slack space.
6. With any drive partition selected from the tree-view the user can view all partition data (cluster by cluster) and any file slack space.

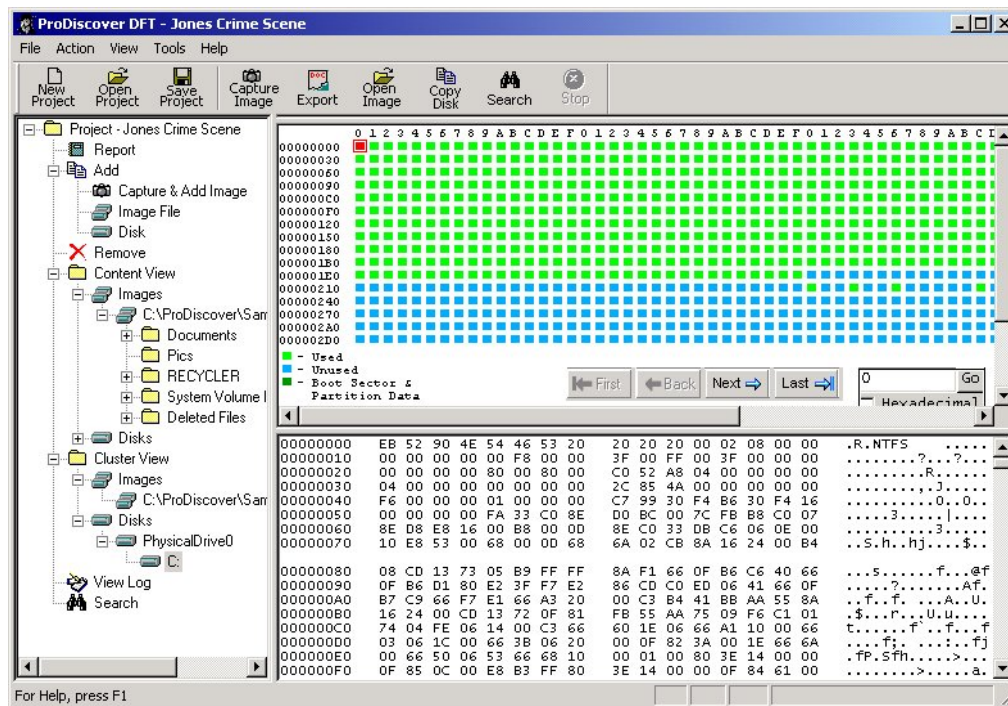
Cluster View of Physical Drive

(Note physical drive selected in Tree View)



Cluster View of Drive Partition

(Note partition selected in Tree View)



Registry Viewer

The registry viewer allows investigators to browse the registry of a Windows system and select individual registry keys as evidence of interest. To process the windows registry ProDiscover needs to read several files on the disk in addition to individual registry files themselves.

To process registry files from the local or remote disk or image users should highlight the windows system directory in content view, right-click and choose "Add to Registry Viewer". The default system directory on a Windows NT 4.0 system is Winnt. In Windows XP the default system directory is Windows. Once the user selects "Add to Registry Viewer" ProDiscover will scan the directory structure and extract the files needed to process the registry view.

EventLog Viewer

ProDiscover allows users to add the Windows Event Logs to a project from images or directly connected disks. Once the event logs are added to a current project, users can review individual log entries and select as evidence of interest if needed.

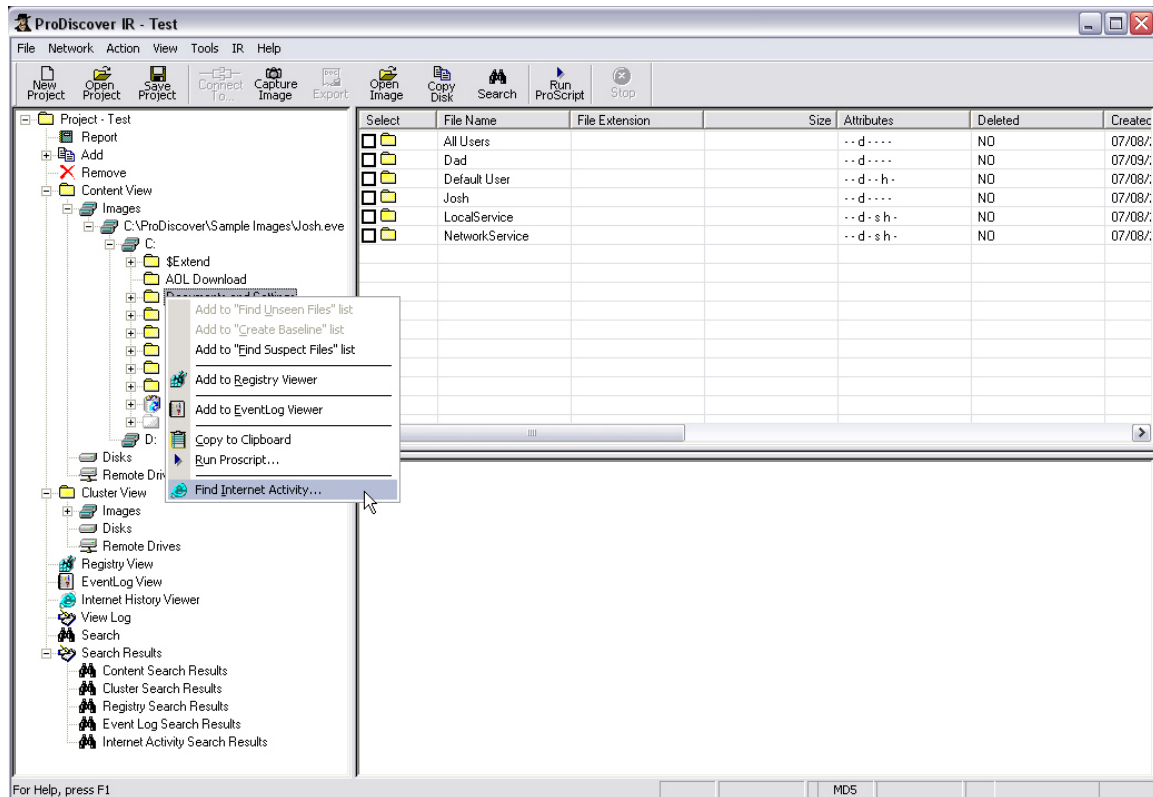
The following steps allow users to add a Windows Event Log to the current project:

1. Add an image file or disk to the current project.
2. Navigate to the Windows installation directory (C:\Windows, C:\Winnt, etc.) on any partition from content view.
3. Highlighting the Windows installation directory from content view, right-click on the directory and choose "Add to Event Log Viewer".
4. The Windows event logs from the selected installation will be available for view from the "Event Log View" tree-view item.

Internet History Viewer

Information about a users Internet Web surfing habits is often crucial to investigations. ProDiscover allows investigators to quickly search for, and extract information from Internet Explorer history files (index.dat). Once the information is extracted it is automatically added to the project report.

searching for and extracting the Internet history from a directly added disk or image is as simple as right-clicking on the desired directory structure and choosing "Find Internet Activity...". ProDiscover will then search the selected directory structure for all index.dat files containing Internet Explorer Web surfing history and populate the Internet History Viewer for further analysis and addition to the project report.



Once complete the Internet History Viewer found in the tree-view will be populated with the contents of each index.dat file created by Internet Explorer. Once added to the Internet History Viewer this information can be searched and added to the project report on an entry-by-entry basis.

View Log

This option will be enabled when either a project file or an image file is opened and displays a log of any I/O errors encountered during a disk capture or copy. ProDiscover extracts the errors related to the images associated with a project and exports them to the project report automatically. Once selected a log selection dialog box is displayed prompting the user to select the image file for which a log file should be displayed. Any I/O errors will be displayed in the work area.



Search

Selection of this item from the tree-view will prompt the user to enter text strings or hex values to search. The user can enter one or more text strings or hex values in the search dialog.

1. The two main search methods available to users are "Cluster Search", which searches every cluster on the selected disk and "Content Search", which searches files by content or name as reported by the selected disks file system. Note that a "Cluster Search" can be time consuming due to the nature of the search, but can return hidden data. When conducting a cluster search users also have the option to automatically extract any clusters containing the search term.
2. When using "Content Search" users can search only within files marked "**Selected**" in "**Content View**" by selecting the corresponding check box.
3. Checking the "Select all matches" checkbox will automatically add all files from the search result to the project report as evidence of interest. Files marked as evidence of interest can be easily copied to review disks using the "copy selected files" option from the tools menu.
4. When using "Content Search" users can search for file names or file content by selecting the corresponding radio button.
5. Search terms should be separated by a new line and can accept wild-cards such as:
 - *.txt
 - *.bmp
 - *.jpg
 - ProductDesign.doc
6. When conducting a content search for patterns ProDiscover will return all words that contained the search term and notify the user of all words found in the search report. For example: A search for the word "Chris" would also return hits for "Christopher". Wild-cards are not recognized when conducting content search for patterns. Users can reduce the number of words found by selecting the "Match whole word" checkbox.
7. The ProDiscover Search Term window can be populated manually or by using the "Load from file..." button. Load from File will take as input any ASCII text file with the file extension .STS and containing search terms.
8. Full Boolean logic operators (**AND**, **OR**, **NOT**) can be utilized when creating search terms. For information on using Boolean operators see the Boolean Search section in Using ProDiscover.
9. Users are allowed to select one or more image file associated with a project. A search can also be performed on directly connected disks that have been added to the current project.

Event Log Search Internet History Search

Content Search Cluster Search Registry Search

☐ Search in Meta Files ☐ Search in Selected Files only

☐ Select all matches

☒ ASCII ☐ Hex

☐ Case Sensitive

☐ Match whole word

☐ Search for files named :

☒ Search for the pattern(s) : Load from file...

Secret AND Confidential
NOT Jones

Select the Disk(s) / Image(s) you want to search in :

C:\ProDiscover\Sample Images\Josh.eve\C:
C:\ProDiscover\Sample Images\Josh.eve\D:

☐ Filter files by Date(s)

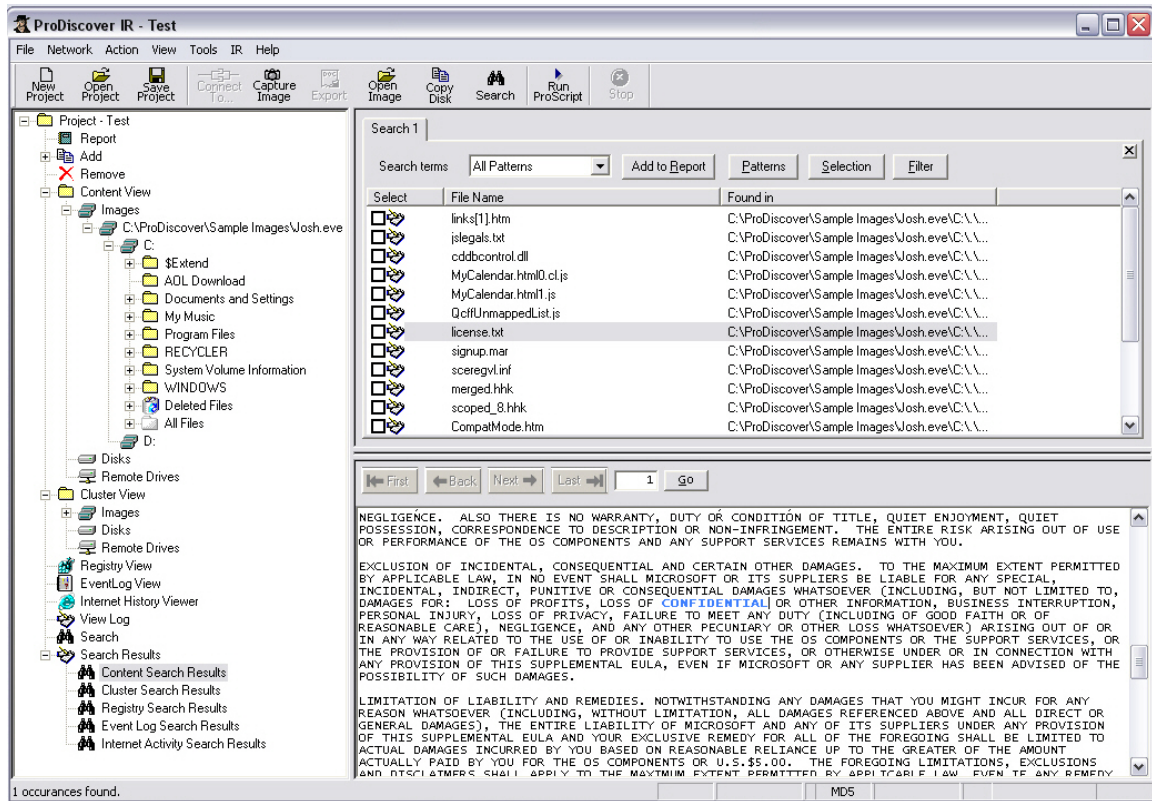
Files ☐ Modified MM - DD - YYYY between

☐ Created and

☐ Accessed

OK Cancel Apply

10. Results obtained from the search will be displayed in the top work area as selectable objects. When any object is highlighted the resulting search term will be highlighted in the data view area. Search results are saved from session to session in a file with the same project name and the extension .ds2
11. If the search results are satisfactory they can be added to the current projects report with the "Add to Report" button.



12. The "Search terms" drop-down box allows users to highlight only a single search term from the original search term list if desired.
13. The "Patterns" button will display a pop-up window containing the original search terms used in the search set including any Boolean operators used.
14. The "Filter" button allows users to filter out files from the search view except the selected term.

File Menu Commands

Options available from the File menu enable the user to start a new project, open an existing project, save the current project, save the current project with another name, open an image file, and exit the program.

The File menu, when clicked presents a drop down menu with the following options, which are described in the links below.

New Project

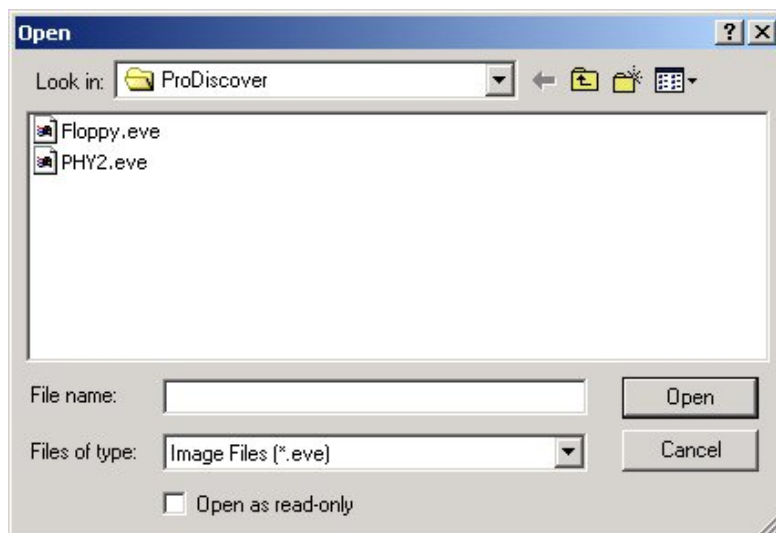
Displays the new project tab (shown below) and creates a new project, as specified by the user, in the main window. New project option prompts the user for a project number, project name and description and creates a template report in the work area.

Open Project

Displays the open project tab (shown below) and opens the project specified by the user in the main window. This opens a file dialog with default extension set to *.dft the default project file extension. When the user selects a valid project file, this loads the file data in the work area.

Open Image

Opens a file dialog allowing the user to select any valid image file. Once selected the action will load the file in the current project.

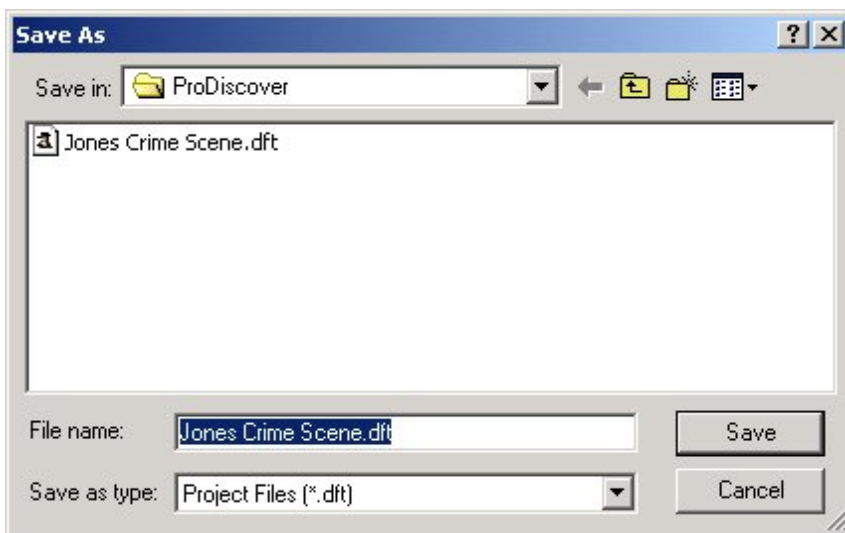


Save Project

Save current environment as a project file with file extension of *.dft. If the project is being saved for the first time then the system displays the File Save As Dialog box and prompts the user to provide a name for the project. The current project will be saved in the default directory. However, the user can navigate to a different directory and save the project in any directory as desired. If the project was saved earlier, then the existing project will be replaced with the current one without any further notice.

Save As

This option functions in a manner similar to the Save option except that, each time the user will be prompted to provide a name for the project. The user can provide a name other than the existing one and save the project as a different file.



Preferences

The preferences menu item found in the File menu launches the preferences dialog box allowing the user to set, or change their personal preferences in any of five areas; General, PDServer, Appearance, Time Zone, and EXIF.

General

The user may select the hashing algorithm utilized by ProDiscover as SHA1, SHA256, MD5 or None. While the SHA256 hashing algorithm is considered by some to be stronger than MD5, there are currently more hash sets available in MD5. Rest assured that MD5 is a very secure method of hashing verification.

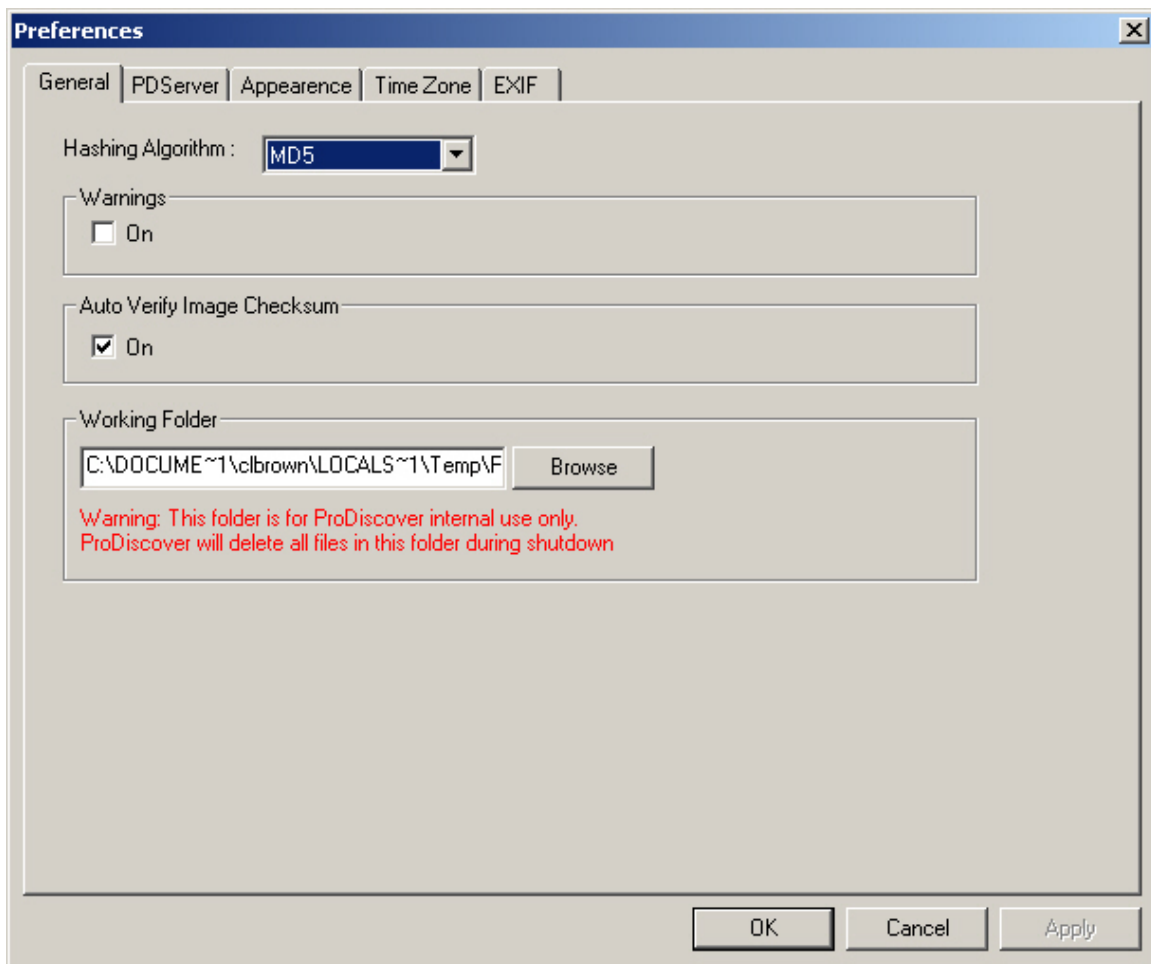
Note while physical disk can freely change hashing algorithm during analysis, images will only support the hashing algorithm selected during capture.

Selecting "None" as a hashing algorithm allows users to select large groups of files as evidence of interest without creating hashes. In cases where large groups of files are being recursively selected, this feature can save time. Once the user desires to add file has values to the ProDiscover report they can change the preferences setting to the desired hashing algorithm, then use "Batch Calculate Hashing..." from the Tools menu to calculate hashes for all files marked "selected" (evidence of interest).

Users may enable warning dialogs that had been disabled earlier and turn on "Auto Verify Image Checksum" to automatically verify image checksums when loading a project or adding an image to a project. **Warning: Turning on "Auto Verify Image Checksum" will cause image addition and project loading to become very slow.**

ProDiscover uses a "Working Folder" to place temporary files in during operations such as generating hash values. By default the "Working Folder" is set to use the current users Documents and Settings temporary folder. Users may select any desired location as the ProDiscover "Working Folder".

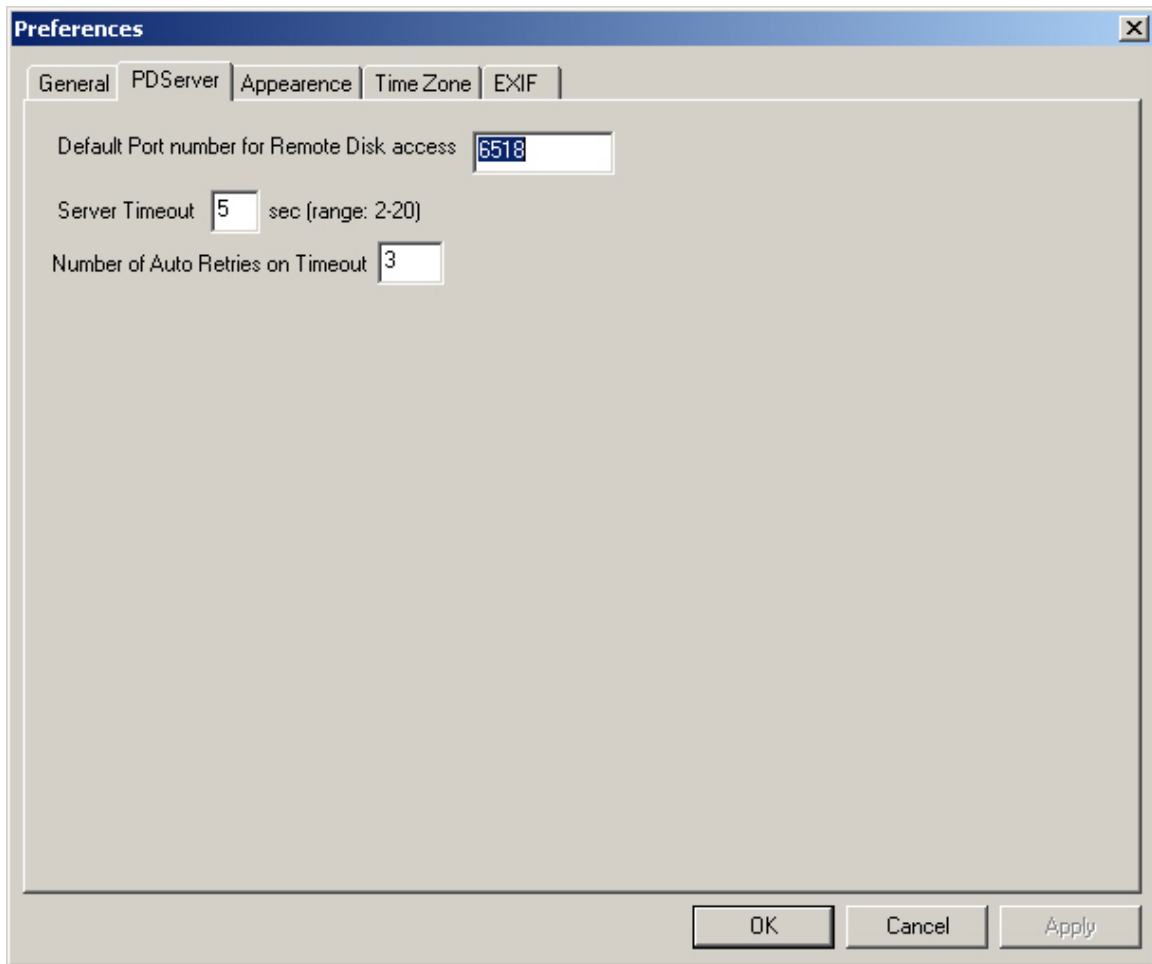
The "When a disk/image cannot be located while opening the project:" setting is primarily intended for users conducting remote investigations. This setting is often referred to as "offline project mode" and includes the choices "Prompt Me", "Add as Offline", and "ignore" Essentially if a user is working a case on a remote system by selecting evidence of interest and adding other artifacts such as search results to the project report all the information is saved in the project file. Prior to version 4.0 the remote disk would need to be accessible for a user to open that previously saved project file. If they had not exported the report they would need to re-connect to the remote disk to do so. There is also other limited functionality a user can perform such as removing evidence of interest.



PDSERVER

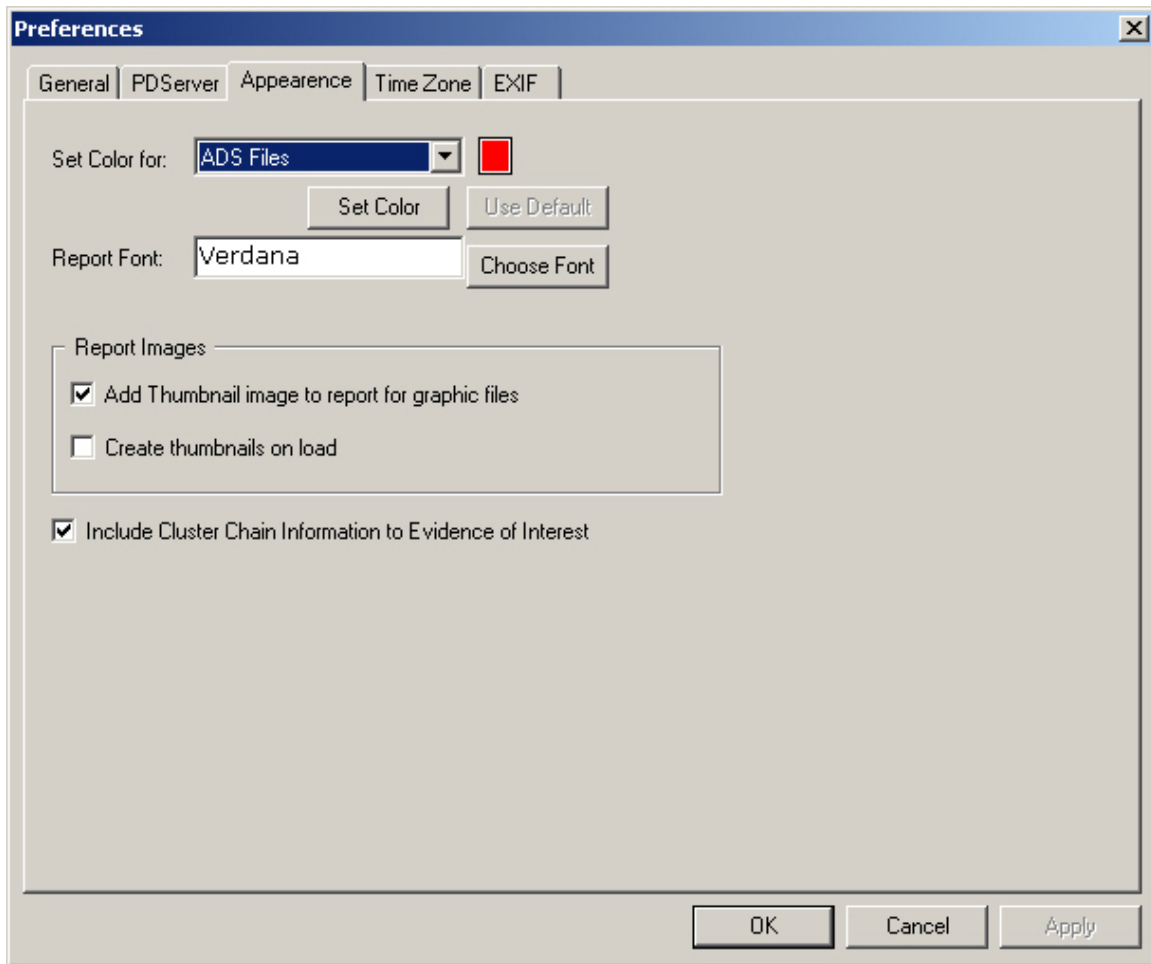
The Default Port number field in the Preferences dialog box allows users to change the default TCP/IP port number used for connecting to remote systems running PDSERVER for network imaging & analysis. Note that if the default port of 6518 is changed on the ProDiscover client the default port number will also need to be changed on the remote PDSERVER. Changing the default port number on the ProDiscover client and server is often helpful in traversing firewalls with inbound and outbound port filtering.

The "Server Time-out" setting tells ProDiscover how long to wait without receiving packets before attempting to reestablish communications with the PDSERVER Remote Agent. The "Auto Retries" setting tells ProDiscover how many times to automatically attempt to reestablish communications after a "Server Time-out" has occurred. Adjusting the PDSERVER "Auto Retries" and "Server Time-out" settings can be helpful for busy networks and Wide Area Networks.



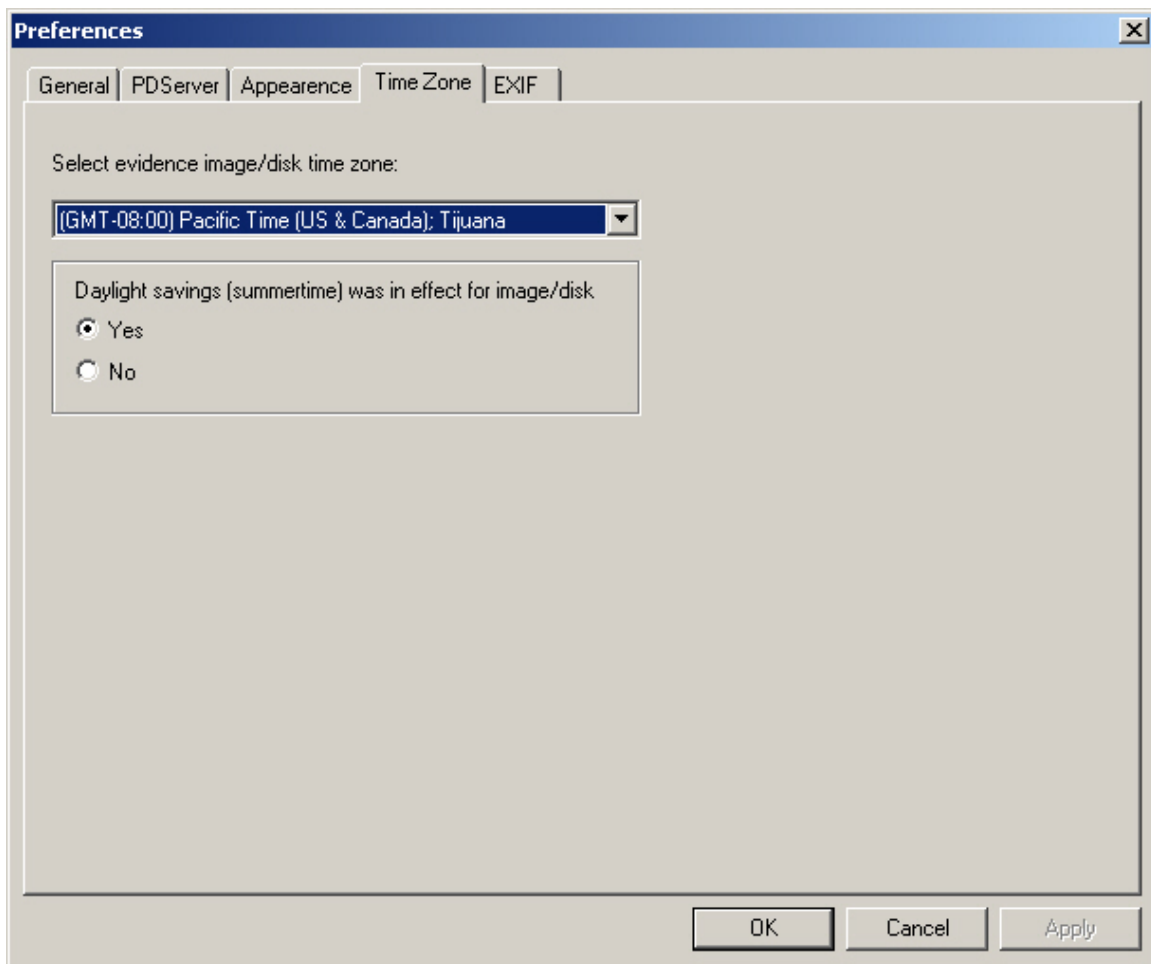
Appearance

The appearance section of the preferences dialog box allows users to set the display color for many file types including files which are marked as the result of hash comparisons and file signature mismatch comparison. Users are additionally provided a facility to change the project report font to any installed system font.



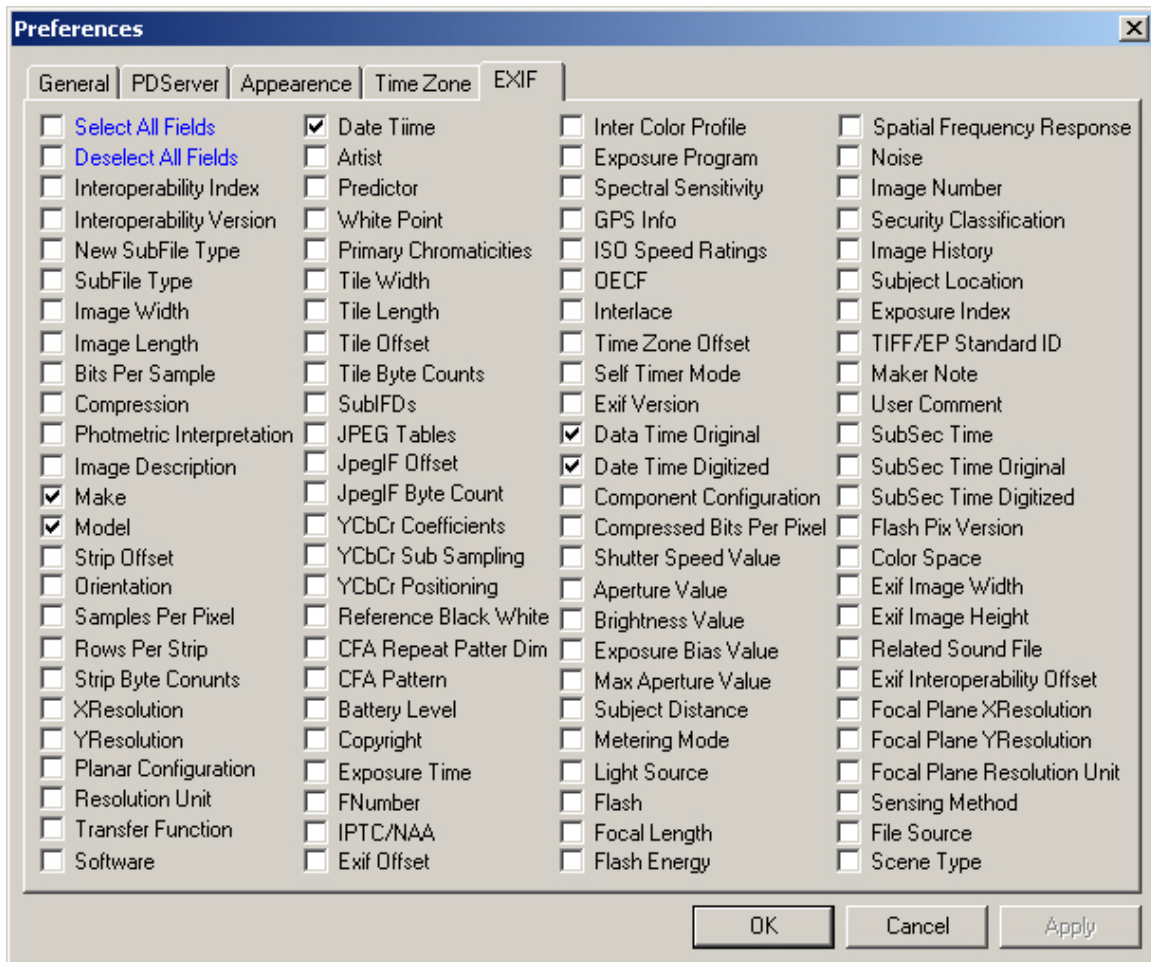
Time Zone

Because the NTFS file system maintains time zone information with files, it is important for investigators to set the proper image or disk time zone information to ensure MAC (Modified, Accessed and Created) times are displayed as they would be on the target system. The time zone preferences dialog allows users to set the ProDiscover time for the disk or image being analyzed. Users can also set whether or not daylight saving time (European summertime) is/was in effect for the disk or image. ProDiscover automatically corrects for a common issue where if users create a file during daylight savings and analyze the file during non-daylight savings, then the files would display times an hour early than actual. Additionally if the opposite happens, then files would display as an hour late.



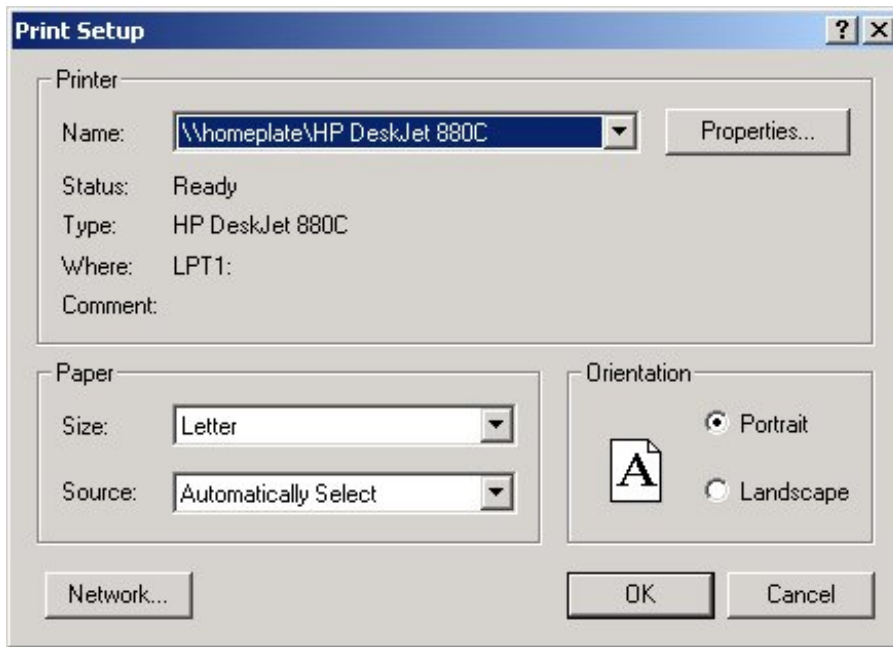
EXIF

Allows users to choose to automatically have EXIF meta data extracted and added to the project report from any image file selected as evidence of interest.



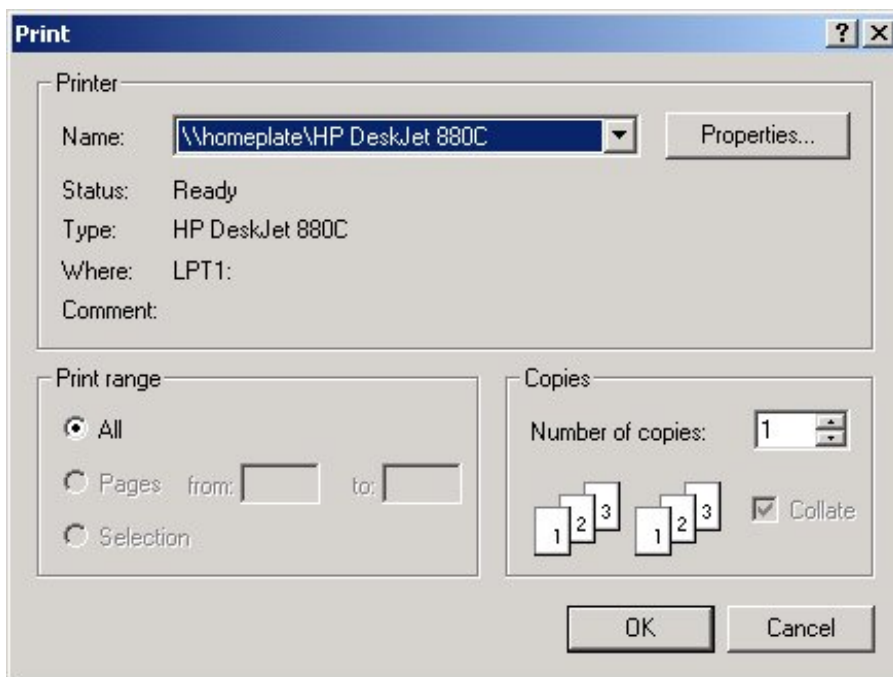
Print Setup

The Print Setup dialog box found in the File menu allows the user to customize printer settings. Use the Print Setup dialog box to change settings such as change the printer selected, paper size and print quality.



Print Report

This option displays a print dialog enabling the user to print the report.



Exit

Allows the user to exit from the ProDiscover program.

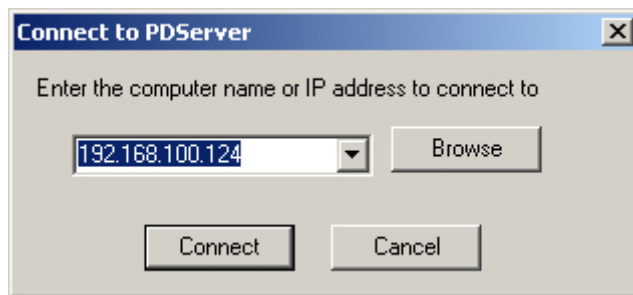
Network Menu Commands

The Network Menu contains options supporting ProDiscover's network imaging & analysis functions. Users will use the Network Menu to perform operations such as connect to a remote **PDServer™** prior to adding a remote disk.

The Network Menu, when clicked presents a drop down menu with the following options, which are described in the links below.

Connect To

Before adding remote disks to a project, users must first establish a TCP/IP connection to the computer running PDServer. Selecting "Connect To..." brings up a connection dialog box with a drop down window allowing the user to select windows computers running on the network. Users can also enter the IP Address of the remote computer directly if desired or if the computer name is not found in the drop-down list.



If the user is connecting to a **PDServer** running in Stealth Mode with a password set the ProDiscover client will display a dialog box asking for the password prior to connection. Even if encryption mode is not set TwoFish encryption is used to create a secure channel for all communications setup to prevent password sniffing and man-in-the middle attacks.

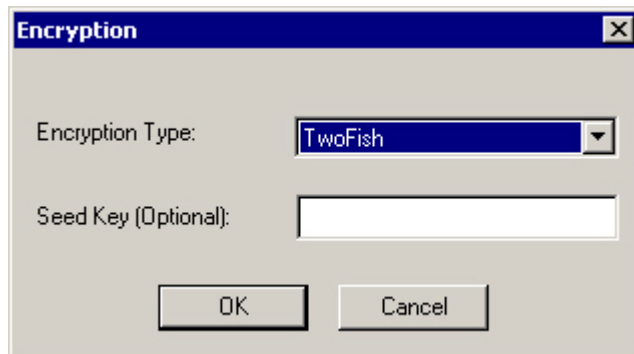


Disconnect

ProDiscover's client/server design allows for only one server and client to be connected at a given time. In some cases users may be running several ProDiscover clients on a network and desire to switch analysis of a single PDServer computer to the other client. In these cases the currently connected ProDiscover client would need to choose "Disconnect" from the network menu first breaking the current connection therefore allowing the second ProDiscover client to establish a connection using "Connect To..." from the network menu.

Encryption

ProDiscover provides encryption to establish a secure channel between the ProDiscover Client and the PDServer for situations where users desire a higher level of evidence spoilage protection. By default encryption is not enabled for performance reasons. By selecting "Encryption" from the Network Menu, users are presented with a dialog box with encryption settings.



By selecting "TwoFish" from the drop-down box and choosing OK encryption will be enabled establishing a secure channel for communications between the client and server. Optionally users can choose their own "Seed Key" used for setting up the encryption channel. If the user does not select a "Seed Key" ProDiscover\ will use its own secret key.

In addition to the TwoFish encryption algorithm, ProDiscover allows users to select 256 bit AES algorithm to secure the data channel.

Even if encryption mode is not set TwoFish encryption is used to create a secure channel for all communications setup to prevent password sniffing and man-in-the middle attacks.

ProDiscover uses the 256 bit TwoFish block encryption algorithm created and analyzed by: Bruce Schneier - John Kelsey - Doug Whiting - David Wagner - Chris Hall - Niels Ferguson. The TwoFish encryption algorithm was one of the selection finalist for the U.S. AES (Advanced Encryption Algorithm) by NIST. For more information about the TwoFish algorithm see the following URL

<http://www.counterpane.com/twofish.html>

Release Remote Client

In some circumstances communications with a PDServer™ remote agent may become disrupted effectively breaking the communications link with the ProDiscover client. If for any reason the link between the ProDiscover client and a PDServer™ remote agent becomes disrupted users may need to reset and release the remote PDServer™. The "Release Remote Client" option found in the network menu will reset any remote PDServer™ agent with which a communications link was previously established.

Action Menu Commands

Options available from the action menu enable the user to accomplish normal application tasks such as: capture an image, add images and disks to a project, search for keywords, export and clear reports.

The action menu, when clicked presents a drop down menu with the following options, which are described in the links below.

Capture Image

Selection of this item from the button bar, or action menu captures bit stream image of the physical drive, partition, or disk group selected based on the inputs provided by the user to password protect and compress the file. Saves the file as an Image file at the destination provided by the user. After an image is captured and written to a file, a hash will be computed allowing the user to verify image integrity.

Note: FAT file systems including FAT32 do not support files larger than 4 MB. Images of drives over 4 MB should be saved to an NTFS, or file system that supports large files.

Capture Image

Source Drive: F:\ [ImageDrive]

Destination: F:\SuspectImage.eve >> Split

Image Format: ProDiscover Format (recommended)

Total sectors to capture : 156296384 HPA

ProDiscover Image

Technician Name: Chris B

Image Number: 039432E

Description :
Suspect Suspect Boot Drive

Compression
☐ Yes
☒ No

Password...

OK Cancel

Disk Groups and Dynamic Disks

Disk Groups are a single disk or group of dynamic disks in Windows NTFS formatted systems. Dynamic disks are physical disks that don't use partitions or logical drives. Instead, they contain only user created dynamic volumes. Dynamic Disks are used to create fault-tolerant volumes such as striped, mirrored, and RAID-5 (Redundant Array of Independent Disks) volumes. Dynamic Disks can also extend volumes and

make changes to the disk without rebooting the computer. ProDiscover supports previewing and imaging Dynamic Disks.

When imaging dynamic disk containing disk groups such as RAID sets, individual disks belonging to the disk group will be captured to different files as physical disks. At the end of the capture, a .PDG (ProDiscover Disk Group) file will be created. The .PDG file contains the information about the image files in the group along with the disk's identifier's for cross-referencing.

Split Images

Users have the option of creating images which are split across two or more files. When selecting to split an image the user can specify each image size or automatically split the images into files of X MB. When ProDiscover creates the split images a ImageName.pds file is also created to maintain information about the split image. When adding a split image to a project users should select the ImageName.pds file and all images will be virtually combined and added to the project.

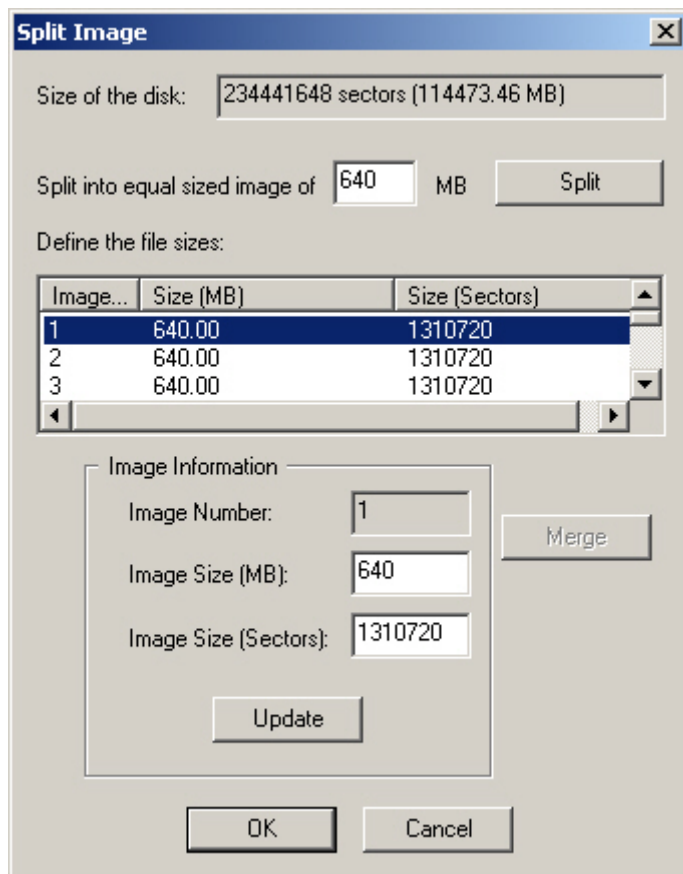


Image Format

Users also have the option to select the desired image format. ProDiscover recommends using the ProDiscover format which includes adding metadata to the image containing information for password protection, time zone, investigator and compression. A technical description of the ProDiscover image format can be found on the Technology Pathways web site in the resources section. Alternately, users can select to create an image in the UNIX style 'dd' format which creates a flat bit-stream image and a corresponding hash file using the selected hashing algorithm. the corresponding hash file will be placed in the image directory and named the same as the image using a .md5 or .sha file extension.

Compression

Images can be compressed to save disk space if needed. Compression is turned off by default for all image captures. To compress the image select "Yes" to compression and ProDiscover will compress the image

and save it as *.cmp. After the image is compressed, if desired, it may be [UnCompressed](#) through the Action menu. Compressed images can be added to any project directly. Compressing an image requires significantly more time to the image capturing process due to the compression overhead.

Password Protection

As an added measure of security, ProDiscover allows user to password protect image files. Users have the option to mask the password, so as not to display the entry to the screen. Once an image is password protected any time the image is accessed the password will need to be entered including opening a project which has the image added to it.

Imaging the ATA Protected area

Often ProDiscover will automatically detect and add file system partitions within the HPA to your directly added disks so they may be viewed as a normal partition in Content-View or Cluster-View. Since the HPA technicle specification does not specify where a file system starts or what type of file system resides within the HPA, ProDiscover provides a tool for scanning the HPA to detect any file systems inside and adding the file system partition to the current project. All file systems added to a project from the HPA will have [HPA] appended in the tree-view to clearly identify their origin. See Using ProDiscover for specific steps and tasks involving the HPA.

Raw Physical Memory and BIOS Imaging

As investigators gain experience, they find the power in simple keyword searching raw data available on disks. These same principles apply to raw data found in a running systems physical memory. Often artifacts such as cached passwords, memory resident only malware, and recently printed documents can be found in physical memory. Another PC artifact of potential value to investigators is a systems BIOS memory stored in NVRAM. Recent advances within the hacker community have demonstrated persistent rootkits stored in this area.

ProDiscover Incident Response and Investigator versions allow investigators to capture image files of both physical memory and BIOS.

Note: information entered in the image capture dialog box is cached during each session to allow faster data entry when capturing multiple images.

Add | Capture & Add Image

Selection of this item from the tree-view, or action menu captures and adds an image to the current project. When capturing the image, this function creates a bit stream image of the drive selected, based on inputs provided by the user, to password protect and compress the file. It saves the file as an Image file at the destination provided by the user. After an image is captured and written to a file, a hash will be computed allowing the user to verify image integrity.

Add | Image

Selection of this item from the tree-view, or Action Menu will display a file open dialog for selection of an Image file to be added to the current project. The file dialog will look for image files with extension ".eve", ".pds" or ".pdg". *.eve is the default ProDiscover image format.

If the image is of a Windows NTFS Dynamic Disk, users should select the image's corresponding *.pdg file which describes the disk group. If the image was a ProDiscover Split image, users should select the *.pds file which describes all split files comprise the total disk image.

UNIX style "dd" images can be added to projects provided with or without the .eve file extension. To add a dd image to the project without an expected extension choose "All Files (*.*)" from the "File of Types" Drop down list. If the "dd" image is split into several images they should be numbered sequentially and all contain a .eve file extension. Once the image files are named and numbered correctly a corresponding *.pds file should be created in the following format:

DD-SplitImage

Split0.eve
Split1.eve
Split2.eve
Split3.eve
Split4.eve

Note that all split image file should be split in sizes which are multiples of 512. To add the split "dd" image users should select the split.pds file created above.

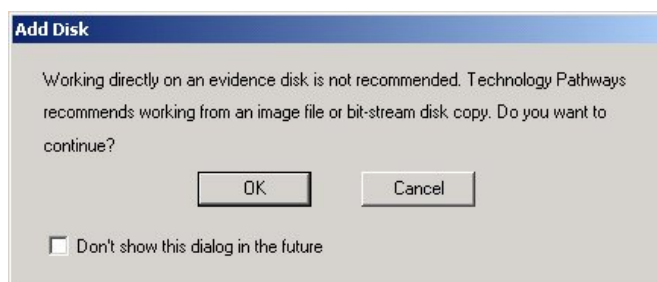
Add | Disk

Selection of this item from the tree-view, or action menu will allow the user to select a hard disk or Disk Group from the local system or system connected through PDServer™ Remote Agent and add it to the project.

Note: Disk Groups are a single disk or group of dynamic disks in Windows NTFS formatted systems. Dynamic disks are physical disks that don't use partitions or logical drives. Instead, they contain only user created dynamic volumes. Dynamic Disks are used to create fault-tolerant volumes such as striped, mirrored, and RAID-5 volumes. Dynamic Disks can also extend volumes and make changes to the disk without rebooting the computer. ProDiscover supports previewing and imaging Dynamic Disks.



Once selecting "Add" you will receive the following warning:



Users can safely disregard this warning if the disk they are adding to the project is a bit-stream image of original evidence and you have installed the image to a system bus with write-blocking capabilities. **Note:** while ProDiscover will not write to any image or drive the operating system will without hardware write-blocking.

It is recommended to use a hardware write-blocking device for analyzing directly attached bit-stream evidence copies. Several such cards widely available are:

- NoWrite™ IDE write blocker (allows ProDiscover access to the Hardware Protected Area "HPA") <http://www.techpathways.com>
- ACARD SCSI-to-IDE Write Blocking Bridge (AEC7720WP) <http://www.microlandusa.com/>
- Intelligent Computer Solutions, Inc. <http://www.ics-iq.com/>

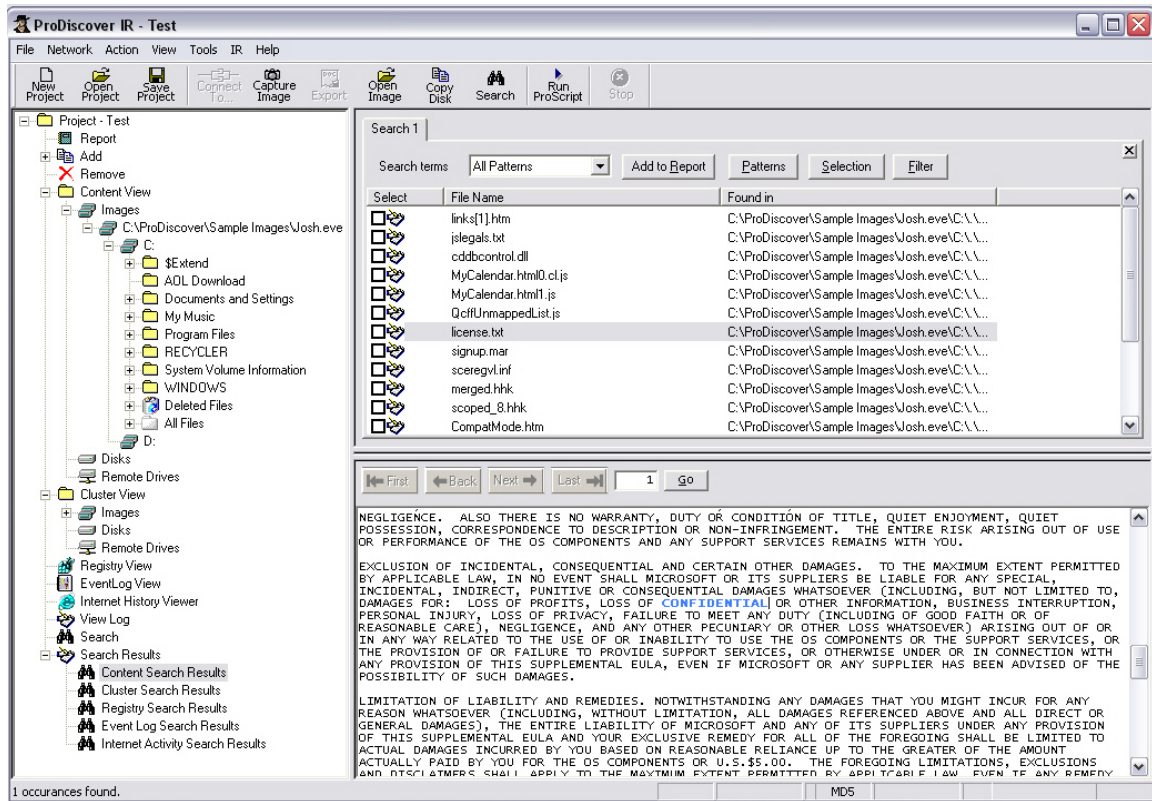
Search –

Selection of this item from the tree-view will prompt the user to enter text strings or hex values to search. The user can enter one or more text strings or hex values in the search dialog.

1. The two main search methods available to users are "Cluster Search", which searches every cluster on the selected disk and "Content Search", which searches files by content or name as reported by the selected disks file system. Note that a "Cluster Search" can be time consuming due to the nature of the search, but can return hidden data. When conducting a cluster search users also have the option to automatically extract any clusters containing the search term.
2. When using "Content Search" users can search only within files marked "**Selected**" in "**Content View**" by selecting the corresponding check box.
3. Checking the "Select all matches" checkbox will automatically add all files from the search result to the project report as evidence of interest. Files marked as evidence of interest can be easily copied to review disks using the "copy selected files" option from the tools menu.
4. When using "Content Search" users can search for file names or file content by selecting the corresponding radio button.
5. Search terms should be separated by a new line and can accept wild-cards such as:
 - *.txt
 - *.bmp
 - *.jpg
 - ProductDesign.doc
6. When conducting a content search for patterns ProDiscover will return all words that contained the search term and notify the user of all words found in the search report. For example: A search for the word "Chris" would also return hits for "Christopher". Wild-cards are not recognized when conducting content search for patterns. Users can reduce the number of words found by selecting the "Match whole word" checkbox.
7. The ProDiscover Search Term window can be populated manually or by using the "Load from file..." button. Load from File will take as input any ASCII text file with the file extension .STS and containing search terms.
8. Full Boolean logic operators (**AND, OR, NOT**) can be utilized when creating search terms. For information on using Boolean operators see the Boolean Search section in Using ProDiscover.
9. Users are allowed to select one or more image file associated with a project. A search can also be performed on directly connected disks that have been added to the current project.

Event Log Search		Internet History Search	
Content Search		Cluster Search	Registry Search
☐ Search in Meta Files	☐ Search in Selected Files only		
☐ Select all matches			
☒ ASCII	☐ Hex		
☐ Case Sensitive			
☐ Match whole word			
☐ Search for files named :			
☒ Search for the pattern(s) :		<input <="" td="" type="button" value="Load from file..."/>	
Secret AND Confidential NOT Jones			
Select the Disk(s) / Image(s) you want to search in :			
C:\ProDiscover\Sample Images\Josh.eve\C: C:\ProDiscover\Sample Images\Josh.eve\D:			
☐ Filter files by Date(s)			
☐ Modified ☐ Created ☐ Accessed MM - DD - YYYY between and			
OK		Cancel	Apply

10. Results obtained from the search will be displayed in the top work area as selectable objects. When any object is highlighted the resulting search term will be highlighted in the data view area. Search results are saved from session to session in a file with the same project name and the extension .ds2
11. If the search results are satisfactory they can be added to the current projects report with the "Add to Report" button.



12. The "Search terms" drop-down box allows users to highlight only a single search term from the original search term list if desired.
13. The "Patterns" button will display a pop-up window containing the original search terms used in the search set including any Boolean operators used.
14. The "Filter" button allows users to filter out files from the search view except the selected term.

Stop Search

This item from the action menu stops any search in progress.

Clear Report | Evidence of Interest

Found under the Action menu | Clear Report, allows the user to clear the current projects report of all evidence of interest that have been added. All other report data will be maintained.

Clear Report | Search Results

Found under the Action menu | Clear Report, allows the user to clear the current projects report of all search results that have been added. All other report data will be maintained.

Clear Report | File Signature Mismatch

Found under the Action menu | Clear Report, allows the user to clear the current projects report of all File Signature Mismatch results that have been added. All other report data will be maintained.

Clear Report | OS Info

Found under the Action menu | Clear Report, allows the user to clear the current projects report of all registry key information that has been added with the OS Info function. All other report data will be

maintained.

Clear Report | Clusters of Interest

Found under the Action menu | Clear Report, allows the user to clear the current projects report of all selected clusters of interest that have been added. All other report data will be maintained.

Clear Report | Unseen Processes

Found under the Action menu, Clear Unseen Processes allows the user to clear information added to the current project report by the IR menu's Find Unseen Processes command.

Clear Report | Registry Keys of Interest

Found under the Action menu, Clear Registry Keys of Interest allows the user to clear information added to the current project report by marking registry keys as selected.

Clear Report | Process List

Found under the Action menu, Clear Process List allows the user to clear information added to the current project report by the IR menu's Get Process List dialog box.

Clear Report | System State

Found under the Action menu, Clear System State allows the user to clear information added to the current project report by the IR menu's Get System State dialog box.

Clear Report | Ports List

Found under the Action menu, Clear Ports List allows the user to clear information added to the current project report by the IR menu's Open/Connected IP Ports dialog box.

Clear Report | All

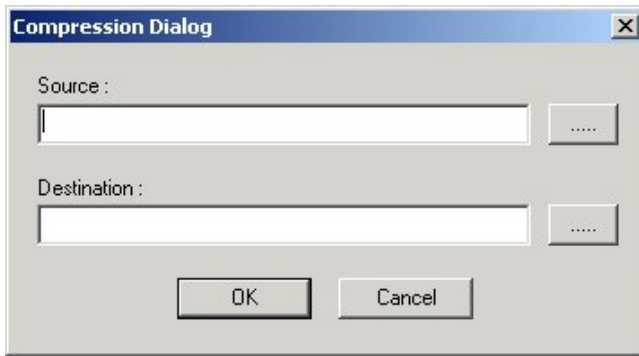
Clears all items within the current project report with the exception of specific object information from any added evidence disk or images.

Clear Recent Projects List

Found under the Action menu, Clear Recent Projects List allows the user to clear all recently opened projects listed under the File menu and the ProDiscover Launch Dialog. This is helpful when you have been working with multiple projects that you no longer intend to work with.

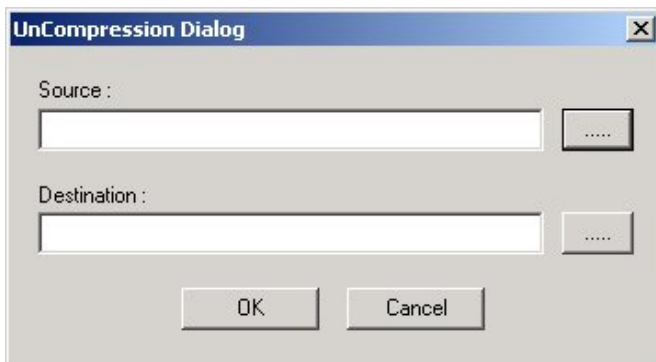
Compress

This feature allows the user to compress an image file that has already been captured. Clicking on the "...." button in the source window will automatically filter out all files but those with .eve extensions within the program directory. All compressed files are saved to the application installation directory with the default extension of .cmp. Compressed images may be added to any working project just as uncompressed images.



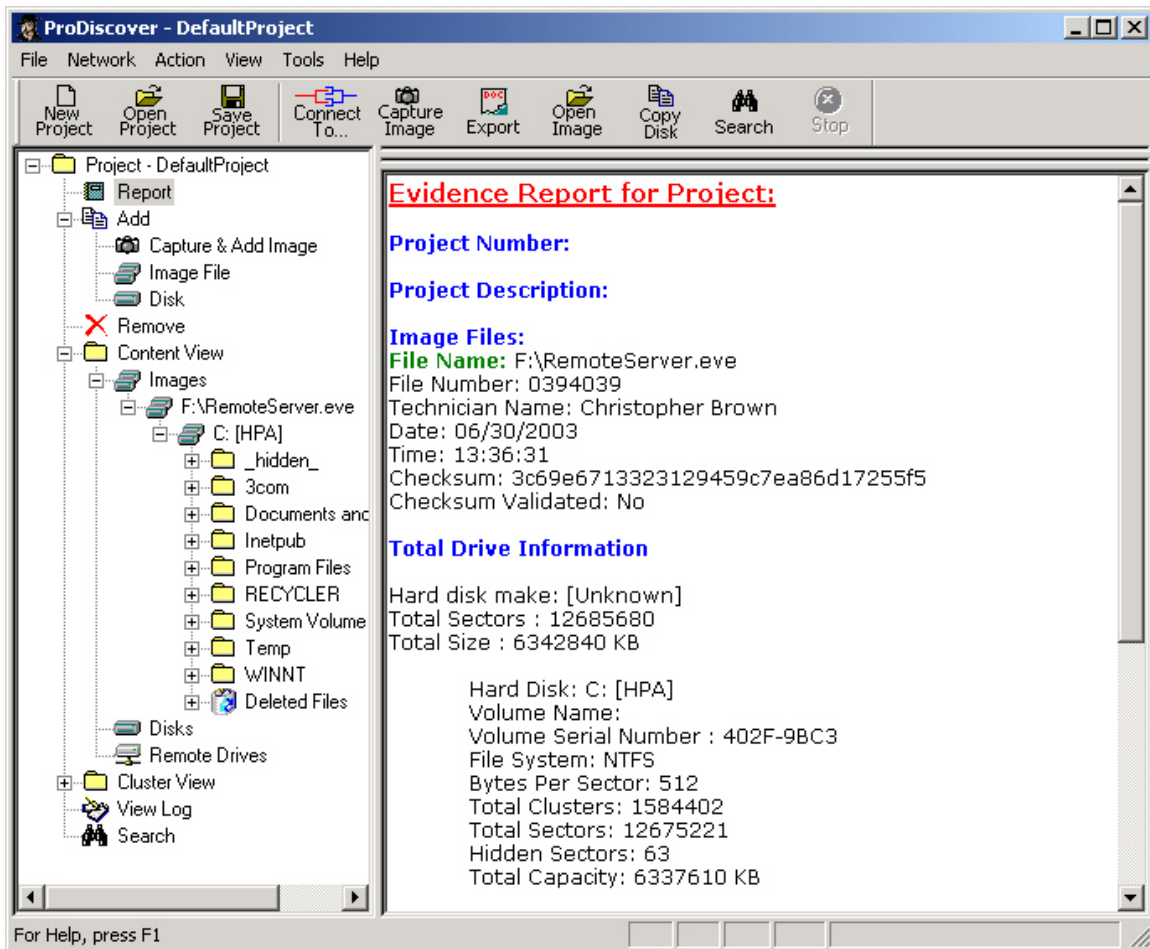
UnCompress

This feature allows the user to decompress an image file that has already been compressed. Clicking on the "...." button in the source window will automatically filter out all files but those with .cmp extensions within the program directory. All image files are saved to the application installation directory with the default extension of .eve.



Export

The Export function found on the button bar and the Action menu, offers the user a convenient way to export the current projects report to a file. Users are given the option to save the report in ASCII Text or Rich Text format. Report files are saved to the ProDiscover installation directory by default. Once exported the report can be edited in the users favorite word processor.



Verify Image Checksum

This item from the action menu allows the user to verify the checksum on an image added to a project. When selected ProDiscover will recompute a checksum for the image and compare the new checksum to the original checksum. Once verified the results will be displayed and the project report updated.

Disk Inventory

The **"Disk Inventory"** option found in the Action menu allows the user to conduct a file and folder count of any disk or image partitions currently selected from Content View.

After selecting any disk root (i.e. the "E:\Images\Image001.eve" just above the partition root "E:\Images\Image001.eve\c:") from content view and choosing **"Action | Disk Inventory"** the disk partitions files and folders will be inventoried with the final count added to the disks or images report section.

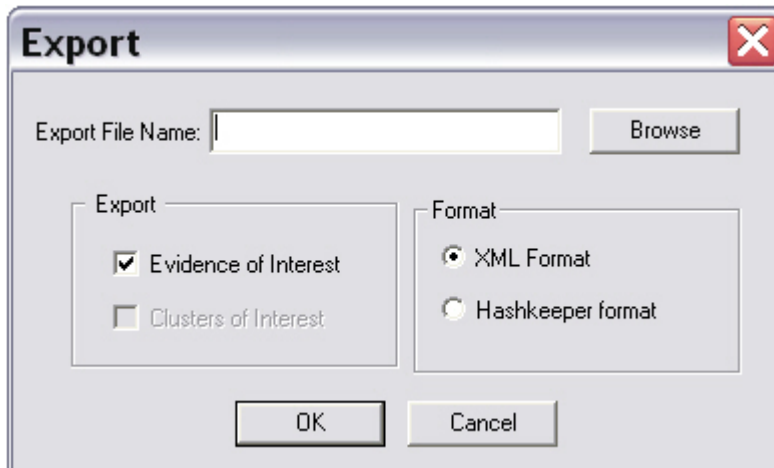
"Disk Inventory results will include Active and Deleted (but recoverable) files and will be displayed in the "Total Drive Information" section of the report "View | Report?"

OS Info

Selecting **"OS Info"** from the action menu with a partition highlighted in **Content-View** will scan the selected partition for Windows registry files. Once the registry files are found they are parsed for Windows installation information. The Windows installation information is then extracted from the registry keys and appended to the current project report.

Export Evidence of Interest

The Export Evidence of Interest allows users to export an index of all items in the current project report which are marked evidence of interest or clusters of interest. When selecting this feature users have the ability to choose the exported index location as well as which items of interest to export. The exported index can be exported in XML or HashKeeper *.hsh format for compatibility with other applications such as Microsoft Excel.



Create report thumbnails

The "Create report thumbnails" menu option allows users to generate and add thumbnail images of graphic evidence of interest after selecting "Add thumbnail image to report for graphic files" in the appearances tab of the preferences dialog box. This menu action is specifically useful when users have recently changed the preferences setting to add thumbnail images to the report, or do not have the "Create thumbnails on load" feature enabled.

View Menu Commands

The view menu enables the user to view the current project report, the contents of image files and disk as files or clusters and I/O log files. Within the view menu the user can also enable or disable viewing of the ProDiscover startup dialog, tool bar and status bar.

The view menu, when clicked presents a drop down menu with the following options, which are described in the links below.

Report

This item in the tree-view and view menu will be enabled only when a project is opened. Selection of this item from the tree-view will display the default project report in the work area with the following headings:

Evidence Report for Project:

Project Number:

Project Description:

Image Files:

Disks:

Evidence of Interest:

File Signature Mismatch:

Search Results:

Project Notes:

Each report heading will be automatically populated during the project session with resulting data from user actions. Enabling a file or directory's "selected tag" within Content View will atomically add that file or directory to the "Evidence of interest" heading within the report. The "Project Notes" heading is a place holder for user notes to be added once the user has exported the report for editing in their favorite word processor.

While working a project, users may find it necessary to clear data within report headings such as, "Evidence of interest" and "Search Results". Removal of data within these headings is easily accomplished using the action menu's "Clear Report - Evidence of Interest and Search Results" function. Removing a disk or image file will atomically remove that items associated information from the report.

Content View | Image

This item in the tree-view and view menu will be enabled only when a project/image file is selected.

Selection of this item from the tree-view or view menu will display the contents of the Image file in the work area. The data files and the folders contained in the disk image captured will be displayed in the work area in a tabular form with information such as: selected tag, file name, file extension, size, modified, accessed and created times, as well as, file attributes. File attribute codes are as follows:

r = Read-only file

a = Archive file

s = System file

h = Hidden file

d = Folder

ADS = Alternate Data Stream File

k = any file that matches a Hashkeeper compare operation

m = any file that contains a signature mismatch after a signature mismatch evaluation if run.

When enabled, the "selected tag" causes ProDiscover to create a cryptographic checksum of the item and insert it into the "Evidence of Interest" section of the project report. Cryptographic checksums are created in the algorithm set by the user in the preferences setting. MD5 is the default algorithm used for checksums. Depending on the processor power available, enabling the "selected tag" can take a few seconds per file due to the checksum creation.

The list shall also include the files marked as deleted by the OS.

Double-click on any file (e.g. file.txt) will display the contents of that file with the default viewer for that type. It is assumed that the default viewer for the file type is available on the machine. If there is no such viewer, a choose application dialog box will be displayed allowing the user to choose an application to view the file with.

Right click on a single file allows the file to be recovered and copied to a destination of choice, including files marked as deleted.

Notes: The "Deleted" column will display "Yes" if the file has been deleted. On NTFS formatted drives, ProDiscover collects all deleted files into a special directory called "Deleted Files" which is not normally present on the original drive. The "Deleted Files" directory is a virtual directory for ProDiscover to recover deleted files in cases where a deleted file can be recovered, but the original path can not be found.

Content View | Disk

This item in the tree-view and view menu will be enabled only when a project/disk is selected.

Selection of this item from the tree-view will be similar to view image file, except that it will display the contents of a directly attached disk which has been added to the current project.

Cluster View

Selection of this item from the tree-view items will display the directly connected disk or an image file as a grid of clusters in the work area with the contents of the cluster in the display area below.

The Zero cluster displays all boot sector and partition data and all subsequent clusters contain actual file system data which are marked "used", or "unused".

The user can easily navigate through the clusters using the navigation buttons below the cluster grid and with left and right mouse clicks.

Selecting an individual cluster will display its contents in the display area in ASCII text and Hex format.

With the physical drive selected from the tree-view the user can view all boot sector and unallocated disk space, as well as all partitions and file slack space.

With any drive partition selected from the tree-view the user can view all partition data (cluster by cluster) and any file slack space.

Cluster View of Physical Drive

(Note physical drive selected in Tree View)

View Log File

This option will be enabled when either a project file or an image file is opened and displays a log of any I/O errors encountered during a disk capture or copy. ProDiscover extracts the errors related to the images associated with a project and exports them to the project report automatically. Once selected a log selection dialog box is displayed prompting the user to select the image file for which a log file should be displayed. Any I/O errors will be displayed in the work area.



Startup Dialog

This option is enabled by default when the user has not checked the "Don't show this dialog in future" option from a new project, open project and recent project dialog. A check mark on the menu item indicates the dialog will be shown.

Tool Bar

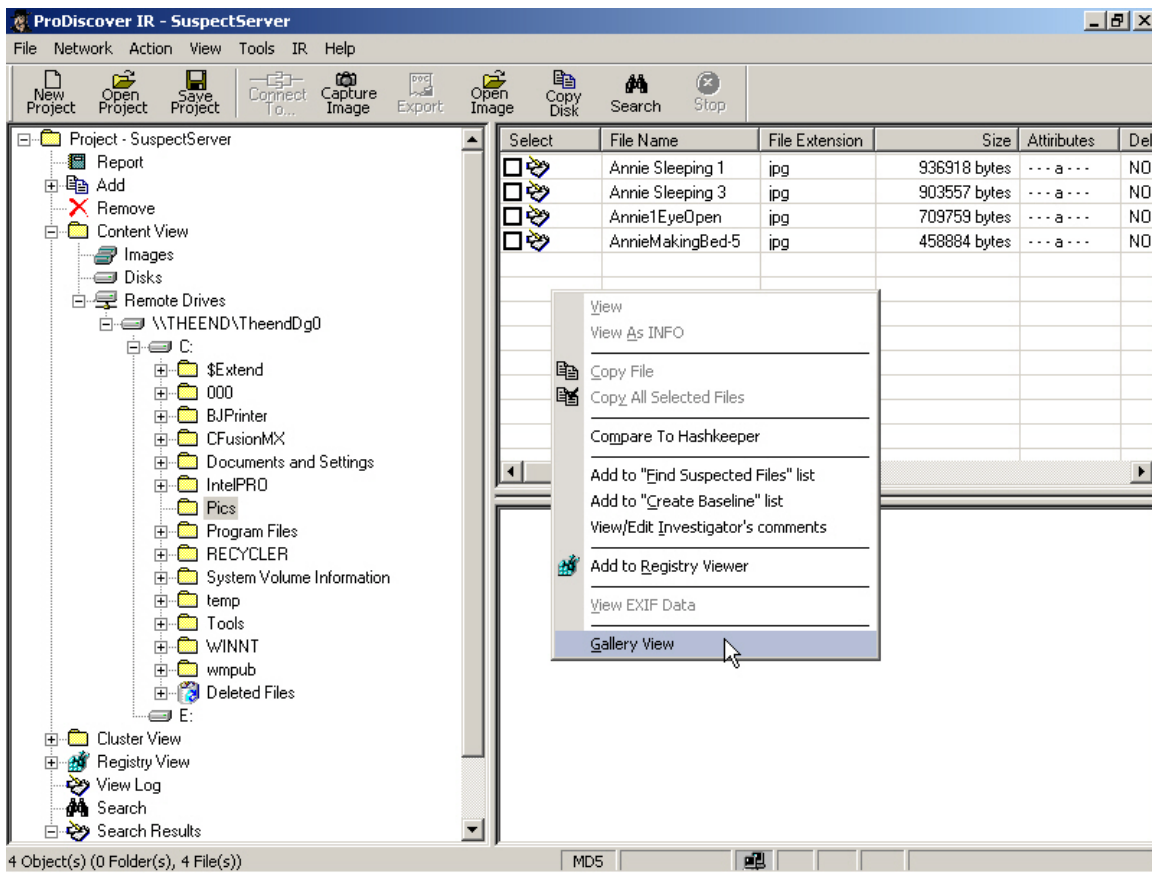
Enables and disables the ProDiscover tool bar.

Status Bar

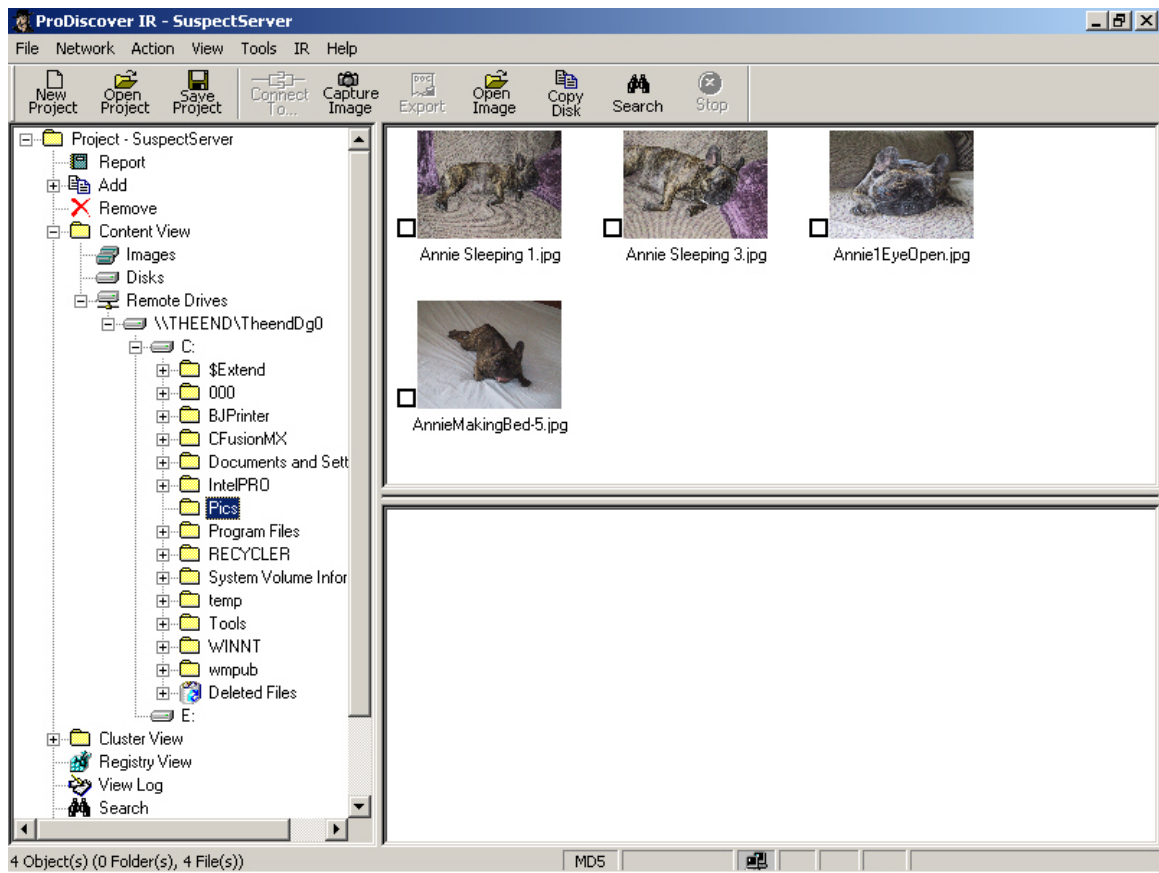
The Status Bar selection found in the View menu allows the user to add and remove the Status Bar from the main window. Users find this helpful when analyzing evidence which requires the maximum amount of screen space possible.

Gallery View

In situations where users need to view the contents of a large number of graphic files in a given directory ProDiscover offers a "Gallery View" function. To shift into a gallery view mode users need only choose the "Gallery View" menu option from the "View" menu or right click over the work area as seen below.



Once the user selects "Gallery View" the work area view will display a thumbnail of all images within the selected directory as seen below.



Tools Menu Commands

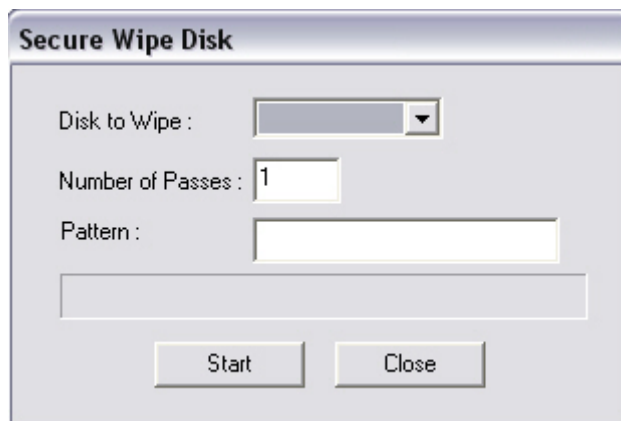
The Tools menu is where the user will find tools such as copy disk and wipe disk.

The tools menu, when clicked presents a drop down menu with the following options, which are described in the links below.

Secure Wipe

ProDiscover implements a The Secure Wipe Disk tool that is designed to meet the Department of Defense clearing and sanitizing standard DOD 5220.22-M. Secure Wipe disk allows the user to image to a target drive that is "Forensically Clean" giving you confidence that your case work will not be jeopardized.

When choosing the Disk to wipe, ProDiscover offers users the ability to wipe a partition or full physical disk. If a partition is selected, ProDiscover will wipe only the file system data in accordance with DOD 5220.22-M. If the user selects the full physical disk, the pattern entered in the "Pattern" window is written to every sector on the disk including any partition and unallocated disk space. If no pattern is entered the ASCII text string "WIPEOUT" is written to disk.



Copy Disk

This option creates a bit-stream copy of one directly connected disk to another directly connected disk. Users may also restore an image file to disk. When this menu option is selected the user will be prompted to select the source disk or image and destination disk.

Note: only physical disk large enough to accommodate the selected source disk will be shown in the destination disk section of the copy disk dialog box.

Windows 2000 users may need to close ProDiscover, Open the Windows 2000 disk manager and write a signature to the target disk before the copied disk is available for addition to ProDiscover projects.

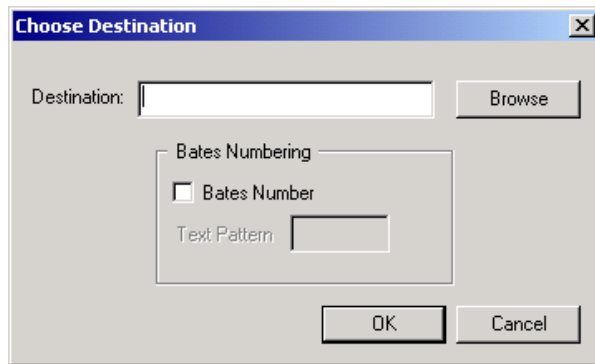
It is recommended to use a hardware write-blocking device for analyzing directly attached bit-stream evidence copies. Several such widely available cards are:

- NoWrite™ IDE write blocker (allows ProDiscover access to Hardware Protected Area) <http://www.TechPathways.com>
- ACARD SCSI-to-IDE Write Blocking Bridge (AEC7720WP) <http://www.microlandusa.com/>
- NoWrite™ IDE Write Blocker. <http://www.TechPathways.com/>

Copy Selected Files

In many cases you will want to recover items to another location in preparation for evidence presentation or further analysis. The "Copy Selected Files" option from the Tools Menu provides users with the ability to conduct a batch recovery/transfer of all items marked as "Evidence of Interest" by enabling the

"Selected" Tag within "Content View".



Bates Numbering

In civil discovery Attorneys use a numbering system to refer to evidence in court called the "Bates Numbering System". With Bates Numbering, each piece of evidence is given a unique number to ensure there is no confusion as to which file is being referred to in court. Computer forensics examiners implement bates numbering when they copy files to CD as evidence in support of civil litigation. ProDiscover Supports the following Bates numbering format originated by Troy Larson.

Example:

Pre-bates file name = MyFile.txt

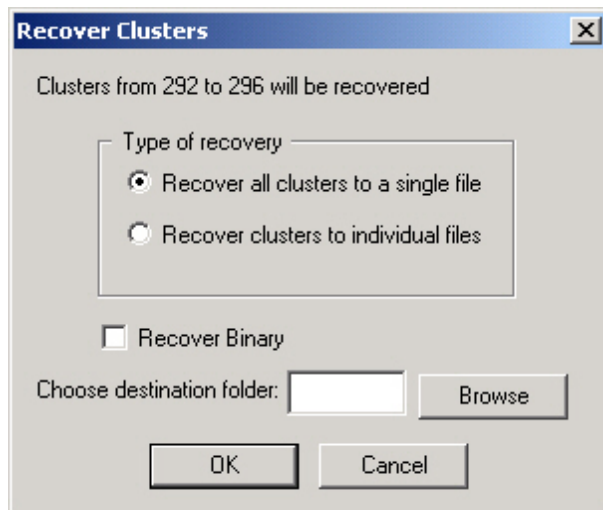
Post-bates file name = MyFile.AAAANNNNN.txt

Where AAAA is up to 4 unique characters string and NNNNN is 5 sequential numbers. The file above might be renamed to "MyFile.EV00001.txt".

In the case where the file had no extension the an extension will be added of ".____" so the file "MyFile" would become "MyFileEV00001.____"

Copy Selected Clusters

In many cases you will want to recover all selected clusters to another location in preparation for evidence presentation or further analysis. The "Copy Selected Clusters" option from the Tools Menu provides users with the ability to conduct a batch recovery/transfer of all items marked as "Clusters of Interest" by enabling the "Selected" Tag within "Cluster Search Results" or "Cluster View".



Filter by Hash Set

ProDiscover creates cryptographic checksums of “interesting files” in popular SHA1 and MD5 algorithms. These checksums can then be compared to known file checksums maintained in the National Drug Intelligence Center (NDIC) Hashkeeper database. The HashKeeper is a database of known file hash values. The database uses the MD5 file signature algorithm to establish unique numeric identifiers (hash values) for known files and compares those known hash values against the hash values of unknown files on a seized computer system. Where those values match the examiner can say, with statistical certainty, that the unknown files on the seized system have been authenticated and therefore do not need to be examined. More information on HashKeeper can be found at www.hashkeeper.org.

TIP:

"Filter by hash set" is a powerful feature which can also be to identify files for which a hash is already known. Many investigators keep hash values in the hashkeeper format for files they often search for. See *the hashkeeper examples installed in the default program installation directory for the hashkeeper file format*. An example of this approach is creating a hash set of known Tootkits or Trojans. Once the hash set is created "filter by hash set" can be used as a search mechanism to find the offending files.

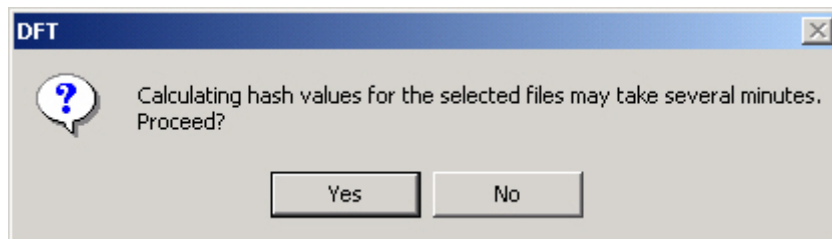
Note that since MD5 and SHA1 file hashes are created for the contents of the file and NOT the file name, hash sets can be used to find known files even when the user has changed the file name.

Batch Calculate Hashing

In some situations users may want to create large indexes of files on a disk without initially calculating a hash value for each file. To add files to the report as "Evidence of Interest" without the hash value the user need only select "**None**" as the hashing algorithm in "Preferences" dialog box (found at File | Preferences).

If later the user desires to create hash values for each file marked "Evidence of Interest" they would set the desired hashing algorithm in the Preferences dialog box then use the "Batch Calculate Hashing..." function found in the "Tools" menu.

Since hash calculation for large groups of files can take some time ProDiscover displays the following dialog box when "Batch Calculate Hashing..." is selected.



Signature Matching

On a windows systems a file signature identifying the type of file is normally contained in the first 20 bytes of the file. For example a Windows Bitmap file with the file extension .bmp would contain "424D" hexadecimal in the first 20 bytes.

Note: The Hexadecimal numbering system, also known as base-16, describes a numbering system containing 16 sequential numbers as base units (including 0). The hexadecimal numbers are 0-9 followed the letters A-F for the 11-16th positions.

File signature mismatch comparison can prove beneficial in filtering data as-well-as, uncovering rudimentary data hiding techniques.

ProDiscover Signature Matching allows the user to compare the file extension to the actual header within the first 20 bytes of the file looking for mismatches. Once a mismatch is found, information about the mismatch including the expected extension can be found in the project report under the heading "File Signature Mismatches". Additionally within the content view, all mismatched files by default will become highlighted in **magenta** and have an "m" added to the file attributes column.

Users can clear file signature mismatch information from the project report by choosing "**Action | Clear Report | File Signature Mismatch**".

TIP: An excellent resource for keeping your file signature database up-to-date is the File Sig web site at www.filesig.co.uk. This site is maintained by Tim Coakley and includes the **filesig** application for managing and exporting file signatures to the ProDiscover format.

ProDiscover provides an easily editable text file with a database of file signatures. The signature database file (headersig.txt) can be found in the ProDiscover installation directory. The file format is as follows:

-----Begin File-----

```
## headersig.txt
## Header Mismatch Configuration File
## On a windows systems file signatures are contained in the first 20 bytes of
## the file.
## Enter headers in the following format:
##
## <File Signature in hex>,<File Extension [s] Separated by ;>,<" Enclosed Signature Name>
##
## Use the # symbol to comment out individual signatures
##
## Many thanks to Tim Coakley, Harlan Carvey, Troy Larson and others who have helped to
create this database.
```

```
FFD8FFFE00, .JPEG;.JPE;.JPG, "JPG Graphic File"
FFD8FFFE00, .JPEG;.JPE;.JPG, "JPG Graphic File"
474946383961, .gif, "GIF 89A"
474946383761, .gif, "GIF 87A"
```

-----End File-----

Scan HPA

Often ProDiscover will automatically detect and add file system partitions within the HPA to your directly added disks so they may be viewed as a normal partition in Content-View or Cluster-View. Since the HPA technical specification does not specify where a file system starts or what type of file system resides within the HPA, ProDiscover provides the "Scan HPA" tool for scanning the HPA to detect any file systems inside and adding the file system partition to the current project. All file systems added to a project from the HPA will have [HPA] appended in the tree-view to clearly identify their origin.

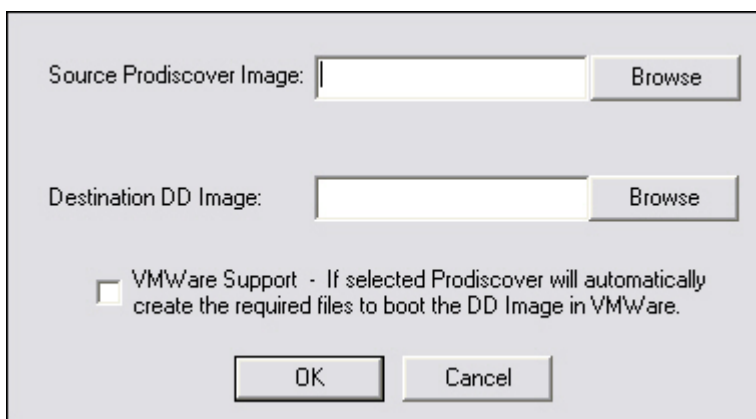
Image Conversion Tools

The "**Image Conversion Tools**" menu option displays several sub-menu items allowing users to convert images to various formats for processing in other tools. The following capabilities are provided:

- Convert ProDiscover Image to "DD"...
- Convert ProDiscover Image to "ISO"...
- Convert "DD" Image to "ISO"...
- VMWare Support for "DD" Images...

Convert ProDiscover Image to "DD"...

The "Convert ProDiscover Image to "DD"..." option found in the tools menu is an image format conversion utility that allows users to create a UNIX "dd" format image from any ProDiscover created image. The source ProDiscover image will be maintained and a new "dd" formatted image will be created as the destination image. Converting images to "dd" format is useful when the user desires to analyze evidence with one of the many tools which support the "dd" format.



As seen in the image conversion dialog box, users are provided the option to create VMWare(r) support files while converting a ProDiscover formatted image to the UNIX DD format.

VMWare 5 offers users to edit the virtual disk file (*.vmdk) to point to a dd formatted image for use in a VMWare virtual machine. This feature allows user to boot an image collected with ProDiscover for investigations that benefit from seeing and capturing the look-and-feel of the suspect system. When the image conversion is completed, users will have an a DD formatted image (image.dd) and a properly formatted .vmdk file (image.vmdk) pointing to the DD image. The simplest way to use these new files in a VMWare virtual machine is to:

Create a new virtual machine in VMWare ensuring that the same image name is given to the virtual disk created by VMWare. If "image" was used for the virtual disk name when creating the virtual machine then the directory containing VMWare files should contain a file named "image.vmdk" after the virtual machine is created.

Copy the newly created ProDiscover image.dd and image.vmdk files to the location the newly created virtual machine files are stored. This process will overwrite the image.vmdk file created by VMWare with the ProDiscover created image.vmdk file.

Configure VMWare as desired and start the virtual machine.

Note: VMWare is a powerful application with many features for maintaining differential analysis and image snapshots that are beyond the scope of this discussion.

A detailed discussion of the conversion process as well as another tool for conversion can be found at <http://www.bschatz.org/2006/p2v/index.html>

A detailed white paper on "VMWare Forensic Cloning Methodology can be found at <http://www.e5hforensics.com/downloads.htm> or <http://www.riskadvisory.net/index.php?id=30>

Convert ProDiscover Image to "ISO"

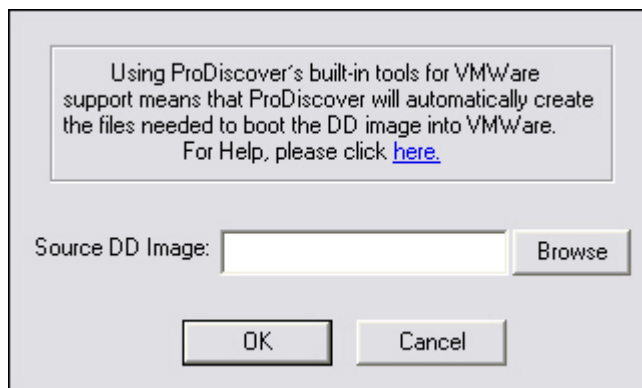
When selected the "Convert ProDiscover Image to "ISO"..." option will convert any ProDiscover formatted image to an ISO 9660 Joliet specifications image.

Convert "DD" Image to "ISO"

When selected the "Convert "DD" Image to "ISO"..." option will convert any "DD" formatted image to an ISO 9660 Joliet specifications image.

VMWare Support for "DD" Images

The "VMWare Support for "DD" Images..." feature is for use when users who captured an original image in DD format desire to create the *.vmdk file for use in a Virtual Machine as described above. Simply provide the location of the DD formatted image and ProDiscover will create a properly formatted .vmdk file for use in VMWare.



Convert Project Format

Beginning with ProDiscover 2.0 project files (*.dft) are in XML format. The "Convert Project Format" utility allows users to convert any project file from previous versions of ProDiscover to the new XML format.

Create remote server disk

The Create Remote Server Disk available from the Tools menu, will generate a PDserver Remote Agent floppy disk when selected. All files are created from the pdserver.eve file located in the \Server directory.

IR Menu Commands (ProDiscover IR Edition only)

The IR menu is available only in ProDiscover Incident Response Edition and provides specialized tools for use in incident response and systems auditing.

The IR menu, when clicked presents a drop down menu with the following options, which are described in the links below.

Find Unseen Processes

The Find Unseen Process operations allows users to scan a remote or local system for files which are locked and running on the system. After ProDiscover determines which files are locked by the system it will compare the list to processes the system "thinks" are running. Both seen and unseen processes will be added to the report.

The Find Unseen Processes operation can provide false positive reports due to file naming or system locking, however all unseen processes should be investigated. The current implementation of Find Unseen Processes is not capable of finding hidden device drivers.

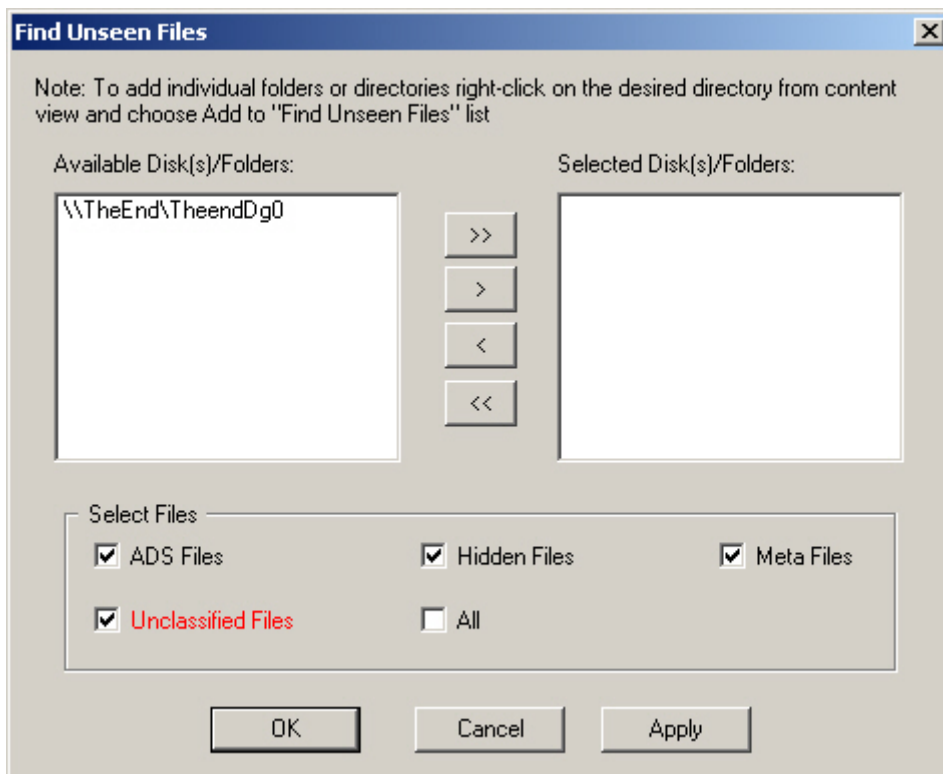
Warning: Users will be presented with a warning dialog notifying them that the "Find Unseen Processes" operation will change last accessed times of folders/directories on the remote system. This operation will NOT change any remote system file last accessed times. The warning dialog box will allow the user to cancel the operation if desired.

Find Unseen Files

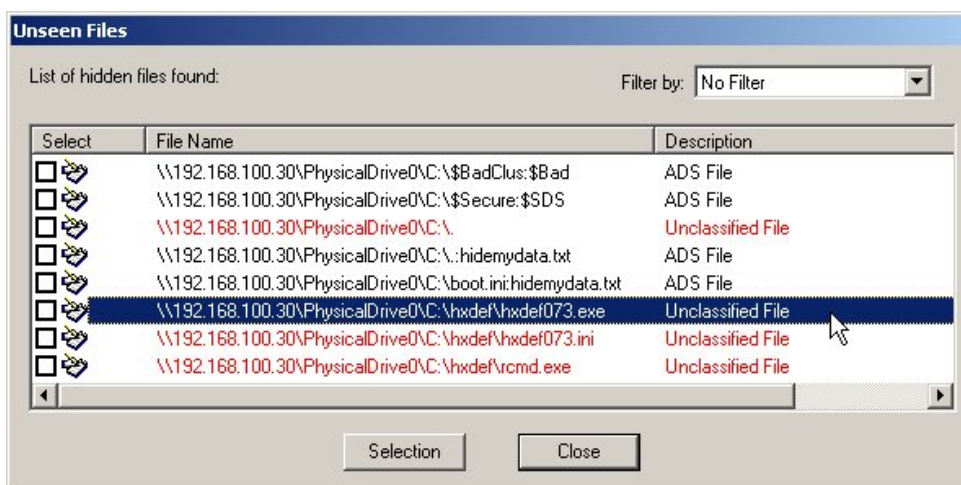
This operation takes a unique approach to quickly detecting hidden files on a remote system without the use of signatures. First ProDiscover will read the file system tables on the remote system from the bottom (bit level) up, then after seeing what is really on the disk the operation will query the remote OS for a complete list of all files it sees. Once the two list are created ProDiscover will compare the two and show all files selected that are hidden from users on the remote system.

Warning: Users will be presented with a warning dialog notifying them that the "Find Unseen Files" operation will change last accessed times of folders/directories on the remote system. This operation will NOT change any remote system file last accessed times. The warning dialog box will allow the user to cancel the operation if desired.

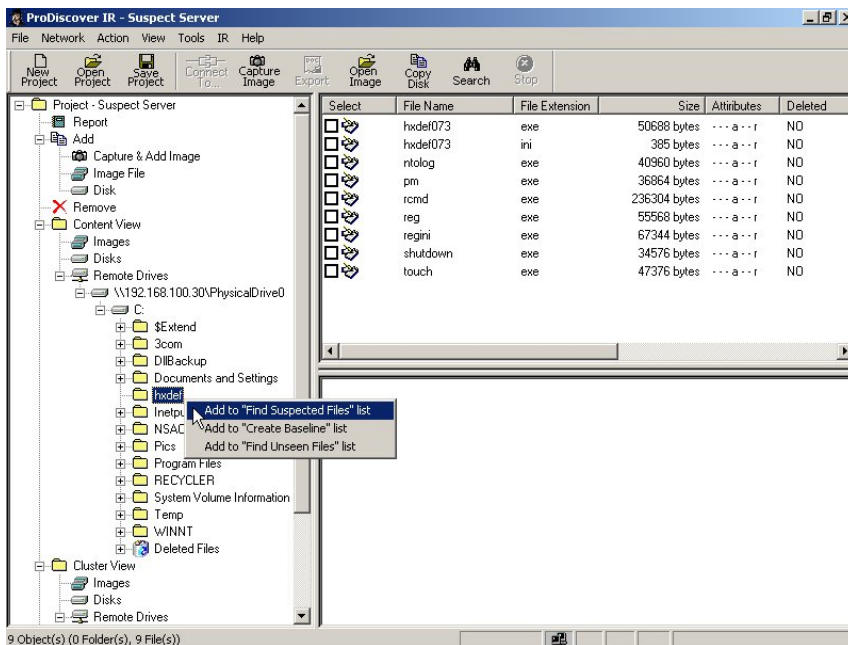
Users are given the option to filter which types of hidden files they desire to identify from a list including ADS (Alternate Data Streams), Hidden Files (Files marked hidden by the file system), Meta Files and Unclassified Files. While users may in certain circumstances be interested in any of these categories, Unclassified files are specifically interesting because this is the category many Rootkits will be found under.



Once the operation is completed the user is shown the results in a pop-up dialog box with all unclassified files highlighted in red. Note the root directory structure \. is always shown in red.

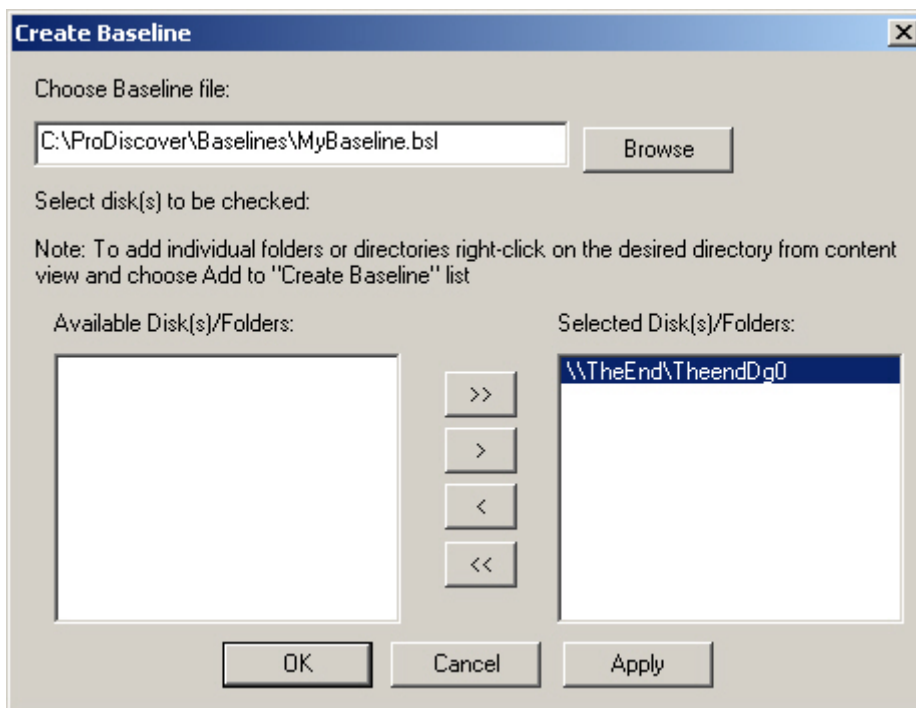


Individual directories can be selected from the tree-view with a right-click action as seen below.



Create Baseline

Administrators who wish to incorporate ProDiscover IR into a comprehensive system integrity verification strategy can use the "IR" Menu options for "Create baseline" and "Compare baseline". Unlike tripwire these features will create a file system baseline hash database from the bottom up (disk bit level) in its read-only file system. From this point on, administrators can conduct an integrity check using the original baseline.

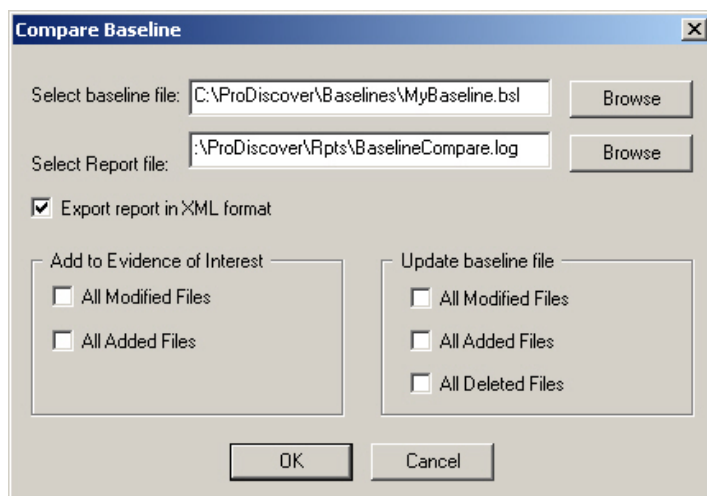


Compare Baseline

The Compare Baseline feature allows users to compare a disk or directory structure's current file contents and hash values against a baseline created earlier and report any additions, deletions or changes.

Once complete a dialog box containing any additions, deletions or changes summary will appear and detailed results will be written to the selected log file. Users have the option of an ASCII text log file (default) or an XML formatted log file.

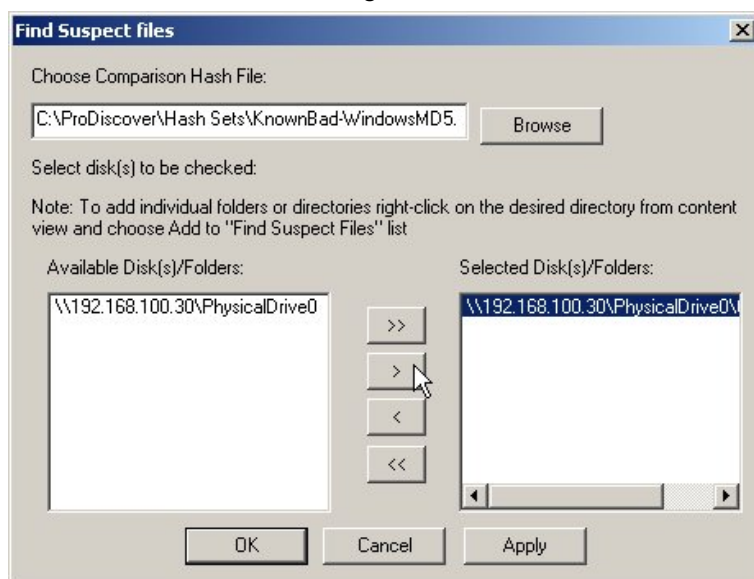
Additionally users have the ability to automatically add any modified or added files to the current projects Evidence of Interest list. To assist in configuration updates, the original baseline file can be updated during the compare baseline if the user chooses.



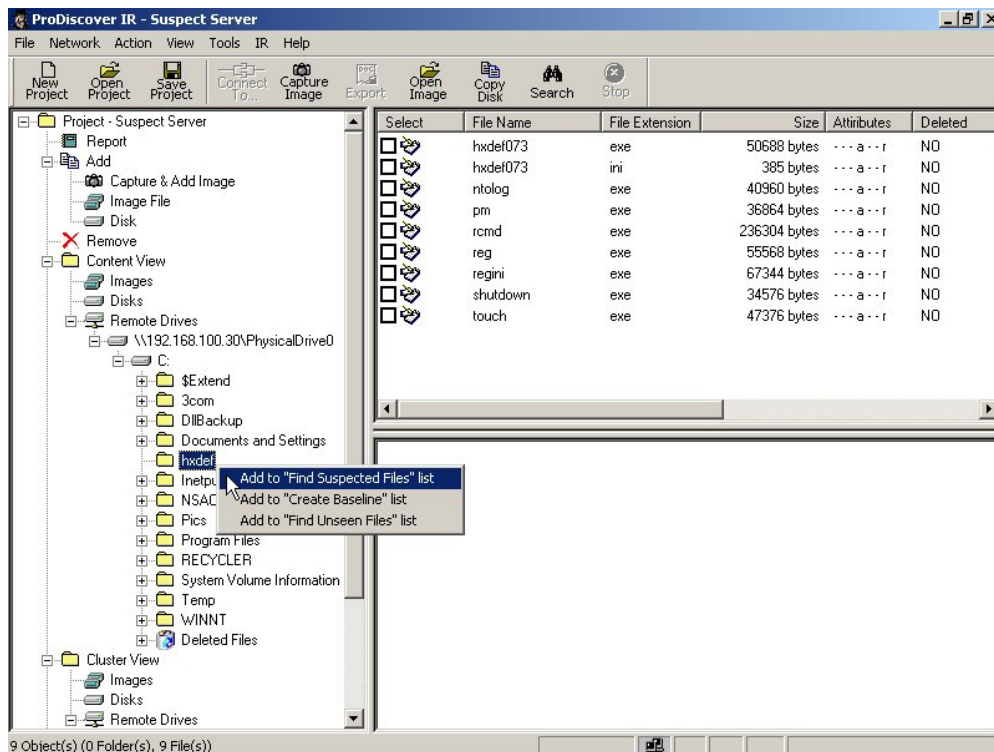
Find Suspect Files

The Find Suspect Files feature allows users to select a directory structure or the entire physical disk and compare the hash signatures against a hash database of suspect or known-bad files. The hash database should be in the NDIC's "hashkeeper" format and have a *.HSH file extension. Technology Pathways provides databases of known-bad and suspect files in the \Hash Sets directory.

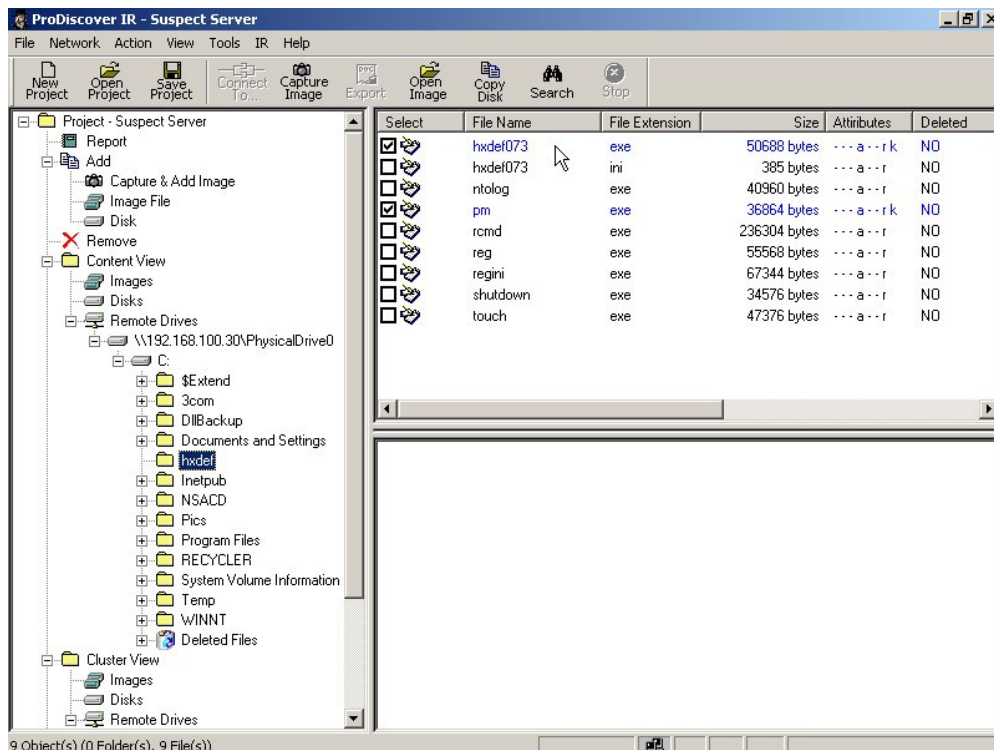
The "Find Suspect Files" feature allows administrators to select an entire disk to scan using the dialog box or individual directories with a right-click from the content-view.



Once the directory or disk is selected the administrator selects any hash database (in Hashkeeper format) to scan and compare against.

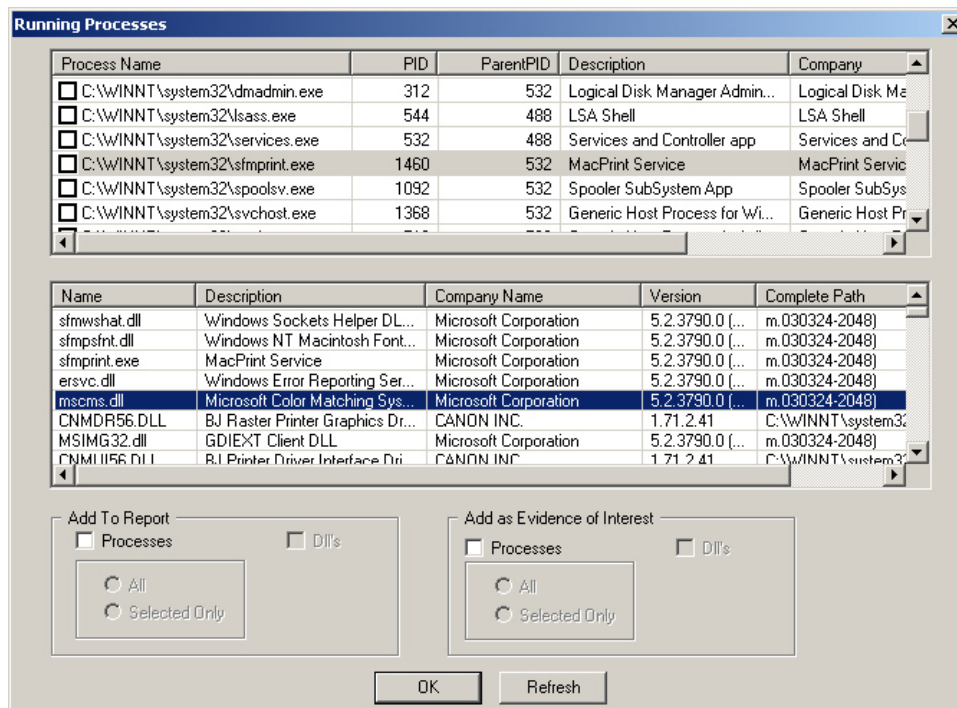


Once the administrator chooses "OK" ProDiscover IR will conduct hashes of all files in the selected directory path using it's read-only, disk-level up file system and then compare the results file-for-file to the selected hash database. The resulting positive matches are then highlighted (blue by default), automatically selected as evidence of interest and added to the project report.



Get Process List

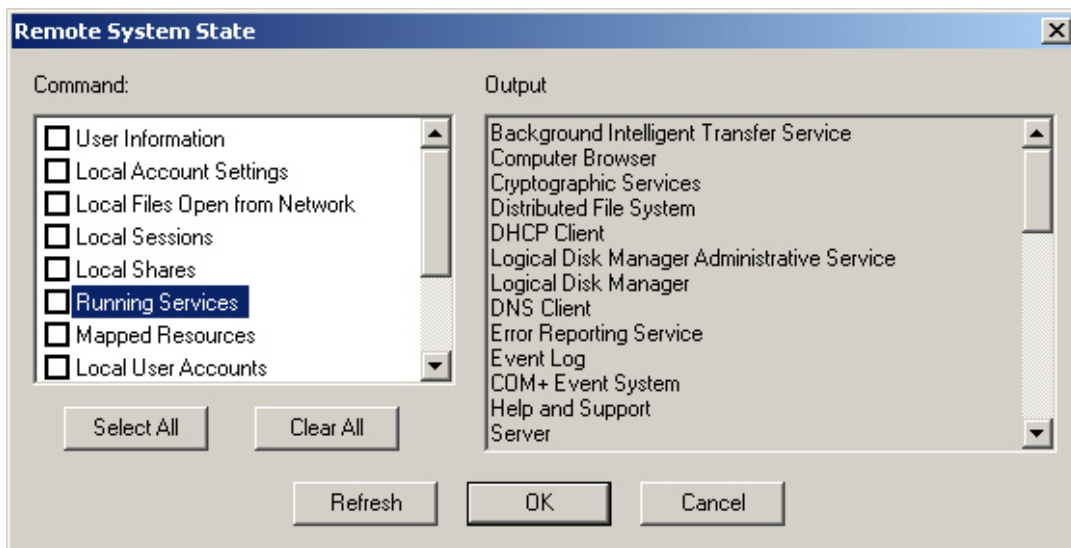
The Get Process List feature available from the IR menu in ProDiscover Incident Response edition allows users to more deeply investigate running processes on a remote system. After connecting to a remote system running the PDServer remote agent and selecting "Get Process List" from the IR menu, the running processes dialog box will appear displaying the running processes on the remote system. After highlighting a specific process in the top view window, all library modules being utilized by the specific process will be displayed in the bottom display window. Users are provided with the capability of adding processes and their dependant dll's (libraries) to the project report and/or adding the process and its associated dll binary file to the report as evidence of interest.



Note: processes hidden by second and third generation rootkits through kernel shimming or dll injection may not be detected by the "Get Process List" function. To detect processes hidden by advanced rootkits users should utilize the "Find Unseen Processes" function from the IR menu.

Get System State

The Get System State feature available from the IR menu in ProDiscover Incident Response edition allows users to gather a great deal of information about the running state of a remote system. After connecting to a remote system running the PDServer remote agent and selecting "Get System State" the remote system state dialog box appears allowing users to identify detailed information about the remote system. From the dialog box, users can select any or all informational items to add to the project report.



Information available from the remote system state dialog box includes:

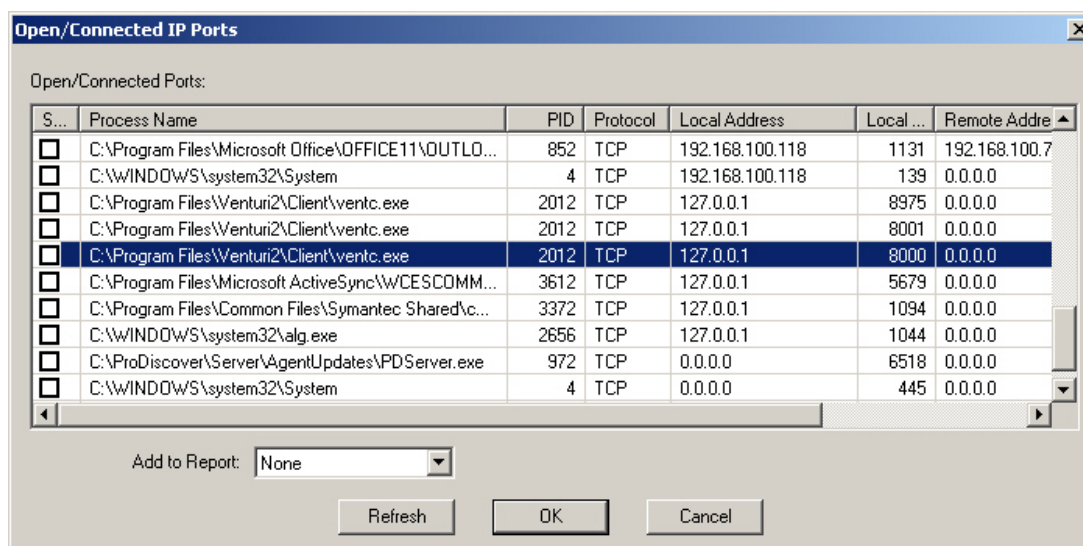
- **User information** - such as the computer name currently logged on user, IP Address and any mapped drives.
- **Local Account Settings** - providing information on user account security settings and workstation role.
- **Local Files Open from the Network** - reporting any system files that are opened for access by remote users.
- **Local Sessions** - displaying any current network sessions open by users remotely including open files, client type, and status of the connection.
- **Local Shares** - shows all local shares including administrative and explicit shares.
- **Running Services** - will display all services running on the remote systems as reported by service manager.
- **Mapped Resources** - reports any remote resources that are mapped to the machine under investigation.
- **Local User Accounts** - displays all local system accounts on the machine under investigation.
- **Locally Seen Computers** - reports all network systems seen to the system under investigation through network browsing.
- **Route Tables** - shows the TCP/IP routing tables in effect on the remote system.
- **ARP Cache** - reports the current address resolution protocol cache contents containing MAC (Media Access Control) address to IP address mapping.

Note: information hidden by second and third generation rootkits through kernel shimming or dll injection may not be detected by the "Get System State" function. To detect processes hidden by advanced rootkits users should utilize the "Find Unseen Processes" and "Find Unseen Files" functions from the IR menu.

Open/Connected IP Ports

The Open/Connected IP Ports feature available from the IR menu in ProDiscover Incident Response edition allows users to gather information about the open and connected IP ports of a remote system.

After connecting to a remote system running the PDServer remote agent and selecting "Open/Connected IP Ports..." the Open/Connected IP Ports dialog box will be displayed showing detailed information about all open and currently connected ports including the status of the connection. Note that on some systems the process id and name mapping may not be available.



Note: information hidden by second and third generation rootkits through kernel shimming or dll injection may not be detected by the "Open/Connected IP Ports" function. To detect processes hidden by advanced rootkits users should utilize the "Find Unseen Processes" and "Find Unseen Files" functions from the IR menu.

Appendix B: Utilizing Boolean Logic in Keyword Search Terms

It is often helpful to utilize Boolean search operators (**AND**, **OR**, **NOT**) to better target search keywords. A good approach is to first think of keywords that best describe your topic. Then combine these keywords using Boolean "operators" to broaden or narrow your results.

ProDiscover provides the letter case specific Boolean operators: **AND**, **OR**, **NOT** as described below.

AND:

The "**AND**" operator tells ProDiscover to search the selected disk, image or disk group for every file or cluster that has each of the words somewhere in the same file or cluster. For example, if you want to find all references a specific project named Philadelphia and the user JJones; you might search the appropriate source in this way:

Philadelphia **AND** JJones

As illustrated above, ProDiscover goes through the selected disk, image or disk group and first retrieves every file or cluster it finds with the word Philadelphia and every file or cluster with the word Jones. It then combines the searches, and gives you only the files or clusters in which both words appear somewhere in the same file or cluster. This is a way of narrowing a search and making it very specific.

OR:

The "**OR**" operator tells the ProDiscover to search the selected disk, image or disk group for every file or cluster which has any of the words specified. Both words do not have to occur in the same file or cluster. For example, if you want information on either a specific project named Philadelphia or the user JJones, you might search the appropriate source in this way:

Philadelphia **OR** JJones

As the search above illustrates, ProDiscover then goes through the selected disk, image or disk group and retrieves every file or cluster with Philadelphia, and every file or cluster with JJones. This results in a very broad search.

NOT:

The "**NOT**" operator allows you to remove a word from your search. It tells the ProDiscover to search for every file or cluster with your first word, and remove any file or cluster which also contains your second word. For example, if you wanted information about the project Philadelphia, but not project information the user JJones worked on, you might search the selected disk, disk group or clusters in this way:

Philadelphia **AND NOT** JJones

As the search above illustrates, ProDiscover goes through the selected disk, image or disk group and retrieves every file or cluster with the word Philadelphia. It then removes any of these files or clusters which also contains the word JJones, and gives you only those records with Philadelphia, not Philadelphia and JJones. The not connector thus narrows your search.

Another useful way to implement the **NOT** operator is to file all files in the selected disk, disk group or clusters which do not contain a specific word such filtering privileged information in civil discovery. For example if you wanted to find all files on a disk that did not contain a specific attorney's name "Smith" you might search the selected disk, disk group or clusters in this way:

NOT Smith

As the search above illustrates, ProDiscover goes through the selected disk, image or disk group and retrieves every file or cluster. It then removes any files or clusters which also contain the word Smith, and gives you all other files or clusters. The not operator thus narrows your search.

Basic Boolean Search Strategy

Identify the concepts in your search.

1. Think of synonyms and alternative ways of expressing each concept.
2. Arrange synonyms for the same concept in a group.
3. Connect your synonyms with "**OR**"s, and place in parentheses.
4. Connect your concepts (or groups of synonyms) with "**AND**"s, or "**NOT**" operators.

Appendix C: Incident Response with ProDiscover IR

Abstract

Given the frequency of alerts from today's Intrusion Detection Systems, most system administrators have experienced that dreaded thought "My system has been hacked!" followed by hours of poking around the suspect file system and log files trying to confirm their suspicions. Let's face it; our security fears in information technology are reinforced on a daily basis by our own experience as well as reports in the media. Based on the 2003 Computer Crime and Security Survey published by the Computer Security institute, only 30% of over 500 companies surveyed indicated they did not experience unauthorized use of their computer systems over the past 12 months. Given the real threats that exist today, a measured approach to investigating suspicious hosts can help administrators maintain their sanity.

This white paper discusses technical incident response methods that can help you quickly evaluate the status of a suspected host. While examples used in this paper focus on Windows hosts, much of the information outlined in this paper will pertain to all operating systems.

Background

For years people have talked about incident response planning and the need for a detailed incident response plan to guide you through difficult procedures in times of confusion. Many of today's incident response guides fail to address steps to assist administrators to adequately verify that an incident has occurred. Furthermore many plans neglect to outline procedures for evaluating an incident in a manner that will properly maintain and preserve evidence for possible future civil or criminal litigation.

You see it over and over again; an administrator suspects a machine has been hacked and they start riffling through the file system looking for anything out of the ordinary. Next they sift through local system logs. Unfortunately, the system administrator can't trust what they see because the system may have been hacked... but they do it anyway. It's the distrust in what they are looking at that causes the administrator to continue to delve deeper into the suspected system trying to find anything that will be conclusive, but the trust issue is there preventing conclusive findings.

Over the years savvy system administrators have developed two methods to help resolve trust issues:

1. Create cryptographic hashes of important files on the file system. In this approach the administrator who suspects a compromised host they can create new hash values and compare the new hash values to a set of "known good" values. (see sidebar)
2. Use a set of known good applications, sometimes referred to as "trusted binaries" to investigate the suspected host running from a CDRom, or remote disk.

Did you know? A Cryptographic hash is an algorithm used to produce fixed-length character sequences based on input of arbitrary length. Any given input always produces the same output, called a hash. If any input bit changes, the output hash will change significantly and in a random manner. Additionally there is no way the original input can be derived from the hash. Two of the most commonly used hashing algorithms are MD5 and SHA1, SHA256.

Unfortunately today's hackers can easily affect a host at a much deeper level than merely replacing files to cover their tracks and set up services. Hackers achieve this deeper infection by installing one of the widely available "Kernel Mode Rootkits". These rootkits are implemented as device drivers in Windows platforms and LKM's (Loadable Kernel Modules) in Linux.

To better understand "Kernel Mode Rootkits" let's take a look at the basic principles of the security kernel architecture used in Windows NT/2000/XP platform design. Microsoft divides the operating system into two modes;

User Mode - This is where all general applications operate. General applications and subsystems for Win32, Win16 and POSIX (Portable Operating System Interface) all run in this mode.

Kernel Mode – This mode is a trusted mode of operation for system services and device operations or access. All requests by user mode applications are brokered through Windows NT Executive Services within the kernel mode. This includes checking security ACL's (Access Control List) and allowing access to file I/O and attached devices.

Did you know? Early rootkits only replaced user mode applications such as "netstat", "dir", etc. By replacing "dir" a hacker could control the "dir" application output (set to not display certain files), but "dir" would still need to request all file I/O from a protected source in the kernel mode. It was these early Rootkits that hashing and trusted binary schemes were designed to overcome.

The current approach to “Kernel Mode Rootkits” is simple. If the goal is to hide a file or process, rather than replace “dir” or “netstat” Why not replace the command user mode applications would call for information from in the kernel? In the case of file I/O we need to replace the kernel mode I/O routine “ZWQUERYDIRECTORYFILE” In this approach not only will “dir” be able to hide hacker’s files, but any other application which makes a call to the kernel mode I/O routine “ZWQUERYDIRECTORYFILE” will receive compromised information. Hackers accomplish this by writing a Windows device driver that through a process called “Hooking” replaces trusted kernel mode I/O routine with their own. Of course the hacker’s routine only provides information they want users to see.

The implication of these relatively new hacking techniques is that comparing hash values of files on the system is useless because any hashes created on the system cannot be trusted. The newly created local hashes would use local system I/O and the user mode files most likely didn’t change anyway. Using trusted binaries running locally will not help for the same reasons.

Another important issue to consider is all that the investigation on the suspect system, even when using trusted binaries from a CDROM, change almost every file’s last accessed time. If it turns out there has been an incident, tracking hacker’s actions becomes more difficult and these changes can raise authenticity issues in legal proceedings.

Resolving Trust in Incident Identification

One accepted way to detect a kernel mode rootkit is to reboot the suspected system in “Safe Mode”, then look around for anything that’s been hiding. Another way is to connect to the suspect system file shares from a trusted remote system (using its [trusted remote system] I/O and trusted binaries) then explore as before. In the first case taking the server offline for mere suspicion is rarely an option. In both cases files last access times will be changed and the question may still remain “are the trusted binaries truly trusted?”

How do you read files from a live systems disks with trusted I/O and not change any last accessed times?

To answer this need Technology Pathways has introduced a new network enabled version of its computer forensics product, ProDiscover IR which reads the live disks sector-by-sector then implements a read-only file system for analysis of the suspect system. See sidebar for a discussion of possible attacks. ProDiscover IRs core features provide the system administrator the ability to investigate suspected systems in a *least-intrusive* manor preserving evidence for possible criminal or civil litigation. Among other techniques the investigation may include searching for known file hash values, recovering deleted files, or searching files and disks for keywords. ProDiscover IR is intended to be a key part of a comprehensive IR investigation including monitoring Intrusion Detection Systems, logging and auditing.

Did you know? Some administrators will suppose that if a rootkit could hook (replace) File I/O request they could simply hook the sector level read commands and foil the approach that applications such as ProDiscover IR use. While this is true on the most basic level, hooking kernel sector read commands would have a trickle-down effect on all other kernel level file system operations and require a large amount of real-to-Trojaned sector mapping and/or specific sector placement for the rootkit and supporting files. This undertaking would not be a trivial task even for the most accomplished kernel mode rootkit author.

For quick and reliable investigations the administrator need only utilize a PDServer™ CDROM or floppy and run “pdserver.exe” on the suspected system. Once PDServer™ is running, the administrator connects to the suspect system from the ProDiscover Incident Response client and adds the suspected disk to a current project. By using ProDiscover in this way, the suspect system can remain up, running, and on-line while the system administrator conducts the examination. The system administrator will see all the files on the suspect system, even files cloaked by Trojans or rootkits, and can access them without altering any valuable data or metadata.

If it turns out after investigation that the server had been compromised, full incident response procedures can be implemented that may included creating a bit-stream image of the suspect hard disk. In this case ProDiscover IR will allow the administrator to create the image through any TCP/IP LAN or WAN in a secure channel encrypted with the 256 bit TwoFish encryption algorithm.

Conclusion

Incident response is a highly procedural process in which identifying an incident alone can be time consuming and require taking critical resources out of service. This impacts overall productivity and if not done quickly, makes it impossible to capture the data needed to catch the criminal. Also, the processes utilized in identifying an incident and capturing “evidentiary quality” data can be critical to successful criminal or civil litigation. ProDiscover IR provides administrators with solutions to quickly identify incidents and properly manage the technical aspects to the corporate Incident Response process.

Detailed Steps to Live Analysis Using ProDiscover® IR

At program launch ProDiscover IR will present a dialog asking the user to create a new project or select an existing project as seen in figure



Figure 1

The user has the option to enter a project number, name, and project description in the new project tab option, then click the **Open** button to create the project. (Note all items are optional with the exception of "Project File Name".)

From the suspect host place a **PDServer™** CDROM in the CDROM drive and execute **pdserver.exe**. Once running, the PDServer™ program window will be displayed as seen in figure 2.

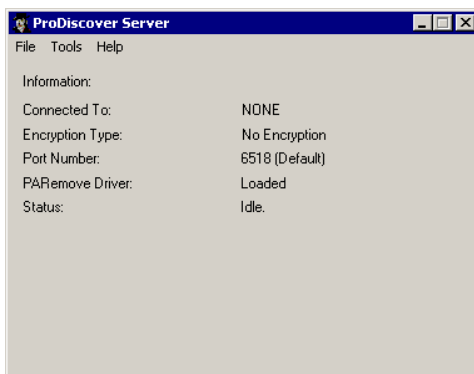


Figure 2

Now that **PDServer™** is running on the remote system, from within an active project on the ProDiscover IR client system use the "**Network**" menu to select "**Connect to...**" and the dialog box seen in figure 3 will appear.

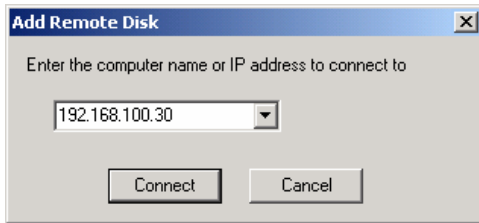


Figure 3

If the user is connecting to a PDServer™ running in Stealth Mode with a password set the ProDiscover client will display a dialog box asking for the password prior to connection (see sidebar). Even if encryption mode is not set, TwoFish encryption is used to create a secure channel for all communications setup to prevent password sniffing and man-in-the middle attacks.

Did you know? “Stealth Mode” is helpful to HR and Policy Compliance Officers desiring to conduct ongoing investigations. “Stealth Mode” prevents the user from knowing the system is being forensically examined. More information on “Stealth Mode” is available in ProDiscover IR documentation.

Once the connection is established, users can create a secure channel if desired by selecting **“Encryption...”** from the ProDiscover clients **Network** menu. If a seed key is not provided, ProDiscover will provide its own discrete key. (see fig. 4)

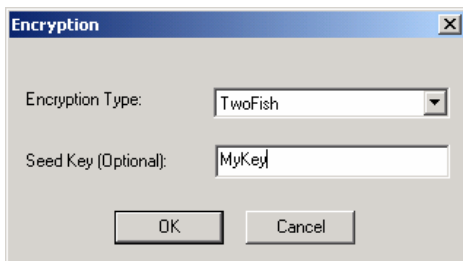


Figure 4

PDServer™ on the remote server will now show the encryption type as seen in figure 5. While encryption does cause some overhead, there is rarely a noticeable difference in performance in most LAN environments.



Figure 5

Once a connection is established the user will choose **“Add | Disk”** or right-click over **“Remote Drives”** in the tree-view and choose the desired remote disk in the dialog that appears. (see fig. 6)

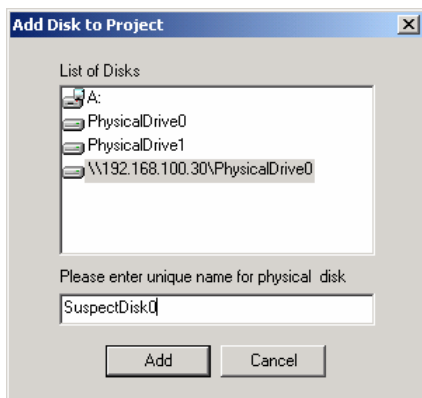


Figure 6

With the remote disk added to the project the user can now browse the file system using the ProDiscover clients content-view item from the left hand program area. (see fig. 7)

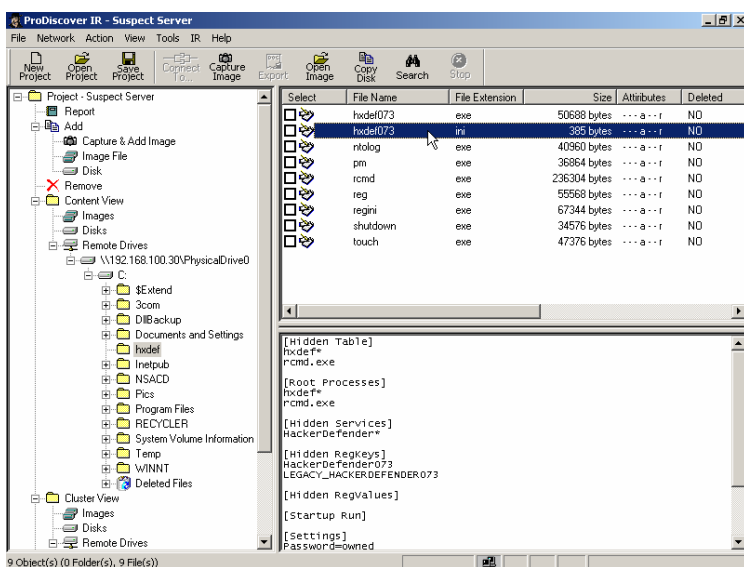


Figure 7

In the case shown in figure 7 the system administrator has found a directory "Hxdef" containing a few suspect files. When selecting the file "hxdef073.ini" the data view area shows the file contents to be alarming. None of these files were visible on the remote system locally or using a trusted binary CD because a RootKit had been installed.

When using ProDiscover IR the administrator can quickly find files hidden from the remote system's users using the "Find Unseen Files" feature available from the IR menu. This process will compare what the file system's low-level file tables contain against what standard file I/O system calls return. To utilize this feature the administrator first selects the directory structure they want to scan along with the types of hidden files they desire to find. (see fig. 8) Individual directories can be selected for comparison by right-clicking on the directory in content view.

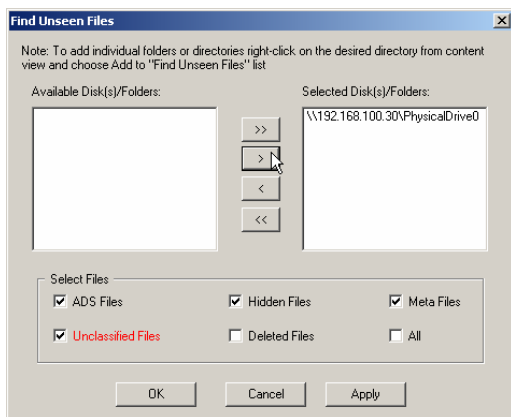


Figure 8

Unclassified Files is where Rootkits normally appear, but administrators may be interested in finding all files marked system hidden as well as ADS files.

The “Find Unseen Files” process is often completed in under ten minutes as seen in figure 9.

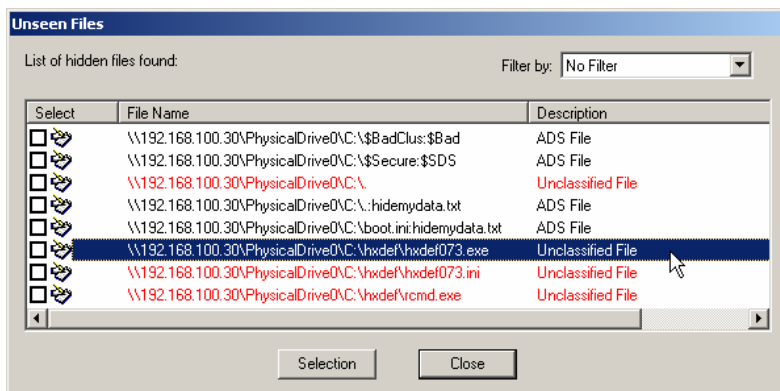


Figure 9

The administrator can select any of the files found in “Find Unseen Files” as evidence of interest and may at this point want to utilize the IR Menu option to “Find Suspect Files” to conduct a more comprehensive file system search.

The “Find Suspect Files” feature offers administrators a method to conduct a comprehensive file hash value comparison against a suspect files list. Technology Pathways provides hash databases for over 400 known bad or suspect files. As when using the “Find Unseen Files” feature, the “Find Suspect Files” feature allows administrators to select an entire disk to scan using the dialog box or individual directories with a right-click from the content-view (fig. 10).

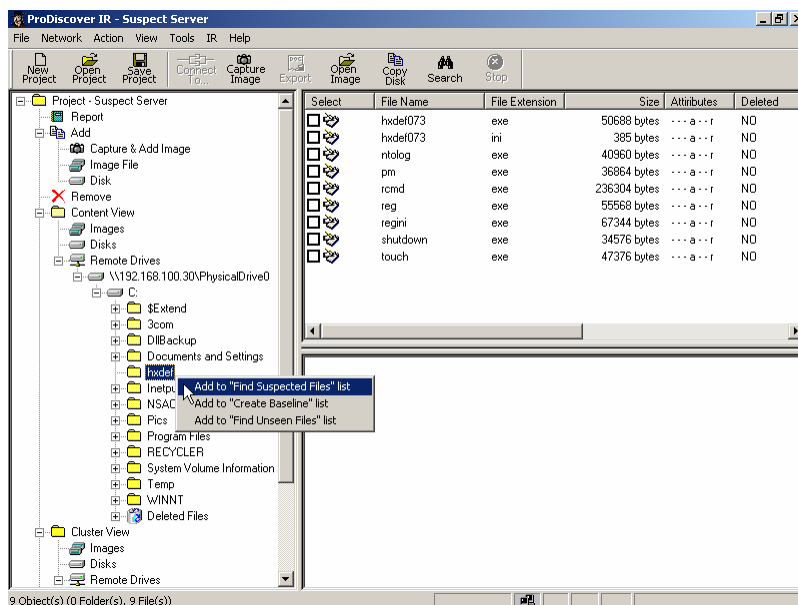


Figure 10

Once the directory or disk is selected the administrator selects any hash database (in Hashkeeper format) to scan and compare against as seen in figure 11.

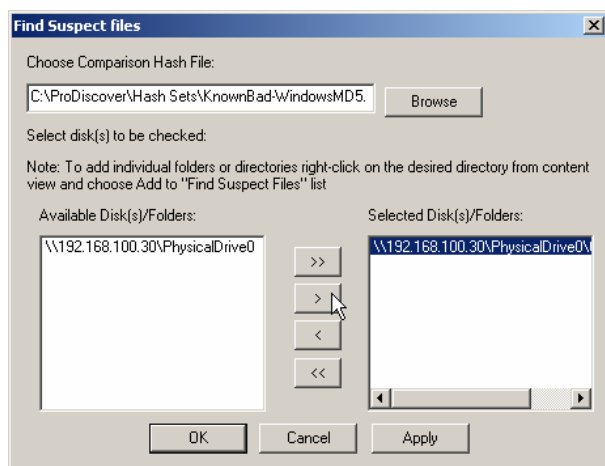


Figure 11

Once the administrator chooses "OK" ProDiscover IR will conduct hashes of all files in the selected directory path using it's read-only, disk-level up file system and then compare the results file-for-file to the selected hash database. The resulting positive matches are then highlighted (blue by default), automatically selected as evidence of interest and added to the project report as seen in figure 12.

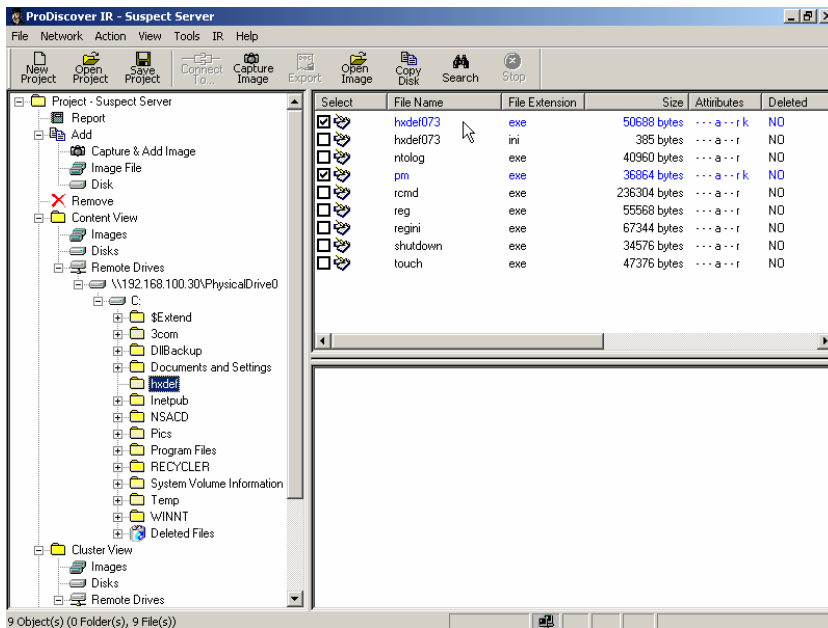


Figure 12

Tip: Administrators who wish to incorporate ProDiscover IR into a comprehensive system integrity verification strategy can use the “IR” Menu options for “Create baseline” and “Compare baseline”. Unlike tripwire these features will create a file system baseline hash database from the bottom up (disk bit level) in its read-only file system. From this point on, administrators can conduct an integrity check using the original baseline.

At this point the administrator knows they have been hacked and can fully implement a incident response plan which most likely includes creating a bit-stream image of the remote system. With ProDiscover the administrator can create the image with a single click on the “Capture Image” icon from the button bar. (see fig. 13)

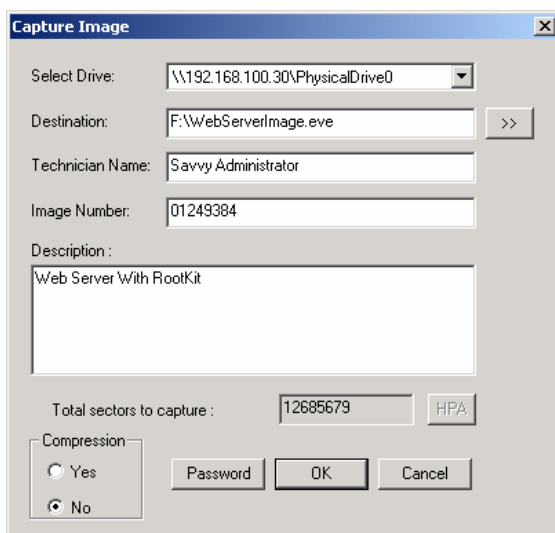


Figure 13

ProDiscover IR provides a variety of other features which fully support accepted computer forensics methodologies as well as the complete incident response process.

Appendix D: Basic Computer Forensics

What is Computer Forensics

To understand Computer Forensics we can start by defining the word "**Forensic**" which can be defined as "Pertaining to the law". With this in mind we can define "**Computer Forensics**" as "the application of computer science to aid the legal process". Computer Forensics is often referred to as Digital Discovery or e-Discovery among legal professionals.

Many professionals perform computer forensics with the intent of aiding corporate policy compliance, or the criminal and civil legal process. These professionals can include:

- Law Enforcement officials
- Legal professionals
- Corporate HR and Compliance Professionals
- Security consultants providing incident response services
- System Administrators performing Incident Response
- Private investigators

Stay Informed

Computer Forensics is as much an art as a science and while common sense will take you a long way, nothing can replace a well informed technician. You will find many means by which to become and stay informed in the References and Resources section of this guide.

Many technicians new to the computer forensics field neglect to develop a good understanding of the legal aspects of forensics sciences prior to performing their first technical investigations. This type of mistake can prove devastating to the case by rendering some, or all evidence collected inadmissible. One of the best guides on the legal aspects of computer forensics is the DoJs Search and Seizure Manual. Of course you should always contact legal representation if you have any questions regarding the legal issues surrounding search and seizure.

Standard Practices & Documentation

While all data collection cases are unique, examiners should develop standard practices and follow them. These standard practices will help ensure that all data collected is collected, analyzed and preserved in the same manner. A publication considered by many as a good guideline for developing standard practices is "The Good Practices Guide for Computer Based Evidence", published by the Association of Chief Police Officers in the United Kingdom.

One of the most important aspects of standard practices is documentation. Documentation of exactly what you did and when you did it during every aspect of an investigation cannot be over emphasized. If litigation occurs as the result of your search and seizure you may be asked to testify as much as a year or more later. Documentation will make this process easier.

Documentation should contain technical aspects of the computer such as operating system settings, BIOS settings, applications installed locally, hardware configuration and user passwords if available.

Additional environment documentation will be needed if the computer seized is installed in a network where servers are utilized for logon, data storage, and applications. This documentation should include logon scripts, policy settings and access rights.

In addition to the technical documentation it is a good idea to keep a running log of your actions and observations. Don't forget to include specific dates and times. This will help you write a summary report if needed later, or be a good memory jogger if you are asked to testify later.

Maintain Chain of Custody

Create a Chain-of-Custody form and manage it vigilantly. The idea behind Chain-of-Custody is simple. Keep track of anyone who has accessed the evidence from this point forward.

Your Chain-of-Custody should include:

1. Who Has physical possession?
2. Why they have physical possession?
3. Where they have physical possession?
4. Any Comments?
5. Signature.

If the evidence is changing possession then the releasing person and the gaining person should sign the document.

Physical Storage

Even if you plan to take the original evidence directly to a work area for analysis, you will eventually need to store the evidence and any copies for safe keeping. Keep all evidence under lock and key and know who has access. Under ideal circumstances only one person will have access to the storage area.

Computer Shutdown

One of the greatest debates surrounding what is known as "Evidence Dynamics" is how to shutdown the computer you are about to seize. Evidence Dynamics can be defined as "Any event that changes or destroys evidence in any way during the processing of the case". Of course there are many other aspects to Evidence Dynamics, but computer shutdown is one of the most actively debated. One side of the debate is if you properly shutdown the computer system with procedures designed for that operating system then you can feel safe that the file system will be kept intact. In some operating systems improper shutdown could damage the file system. The other side of the debate is the school of thought that the suspect computer could be "rigged" to go through a series of file damaging procedures if not shut down in a special way. It is because of this that some security professionals recommend pulling the plug. Considering that even if a minor amount of file integrity is lost due to an improper shutdown, bit stream analysis of the drive would not be hindered. Additionally, on a windows NT/2000 system, registry settings can be made to flush the page file upon shutdown, which may remove valuable information in its self.

No matter how you look at it, there is no correct answer. The best answer will be based on experience, type of operating system and an understanding of other mitigating issues.

Imaging Evidence Drives

It has long been standard practice within the computer forensics community to use some type of imaging technique to image original evidence drives for subsequent analysis. Some benefits to this technique include:

1. Limiting access to original evidence.
2. Allowing technicians to run the imaged evidence environment without risk of modifying the original evidence.
3. Allowing technicians to use a variety of analysis tools on the imaged evidence without risk of modifying the original evidence.
4. Saving time by allowing multiple technicians to perform analysis on multiple images of the original evidence.

No matter how you look at it, working on an image is a good idea. The key to successful imaging and analysis of an evidence disk is to ensure that you can attest that the results have not been modified, or do not vary. It is recommended that you create a bit stream image of the evidence drives utilizing forensics software that meets the mandatory requirements and assertions found in version 3.1.6 of the NIST Disk Imaging Tool Specification, such as ProDiscover.

Points of note to enhance evidence integrity include the following:

- Utilize a new shrink-wrapped drive for the image, or a DOD wiped drive, a process often referred to as using a "forensically clean" drive.
- Ensure a cryptographically or mathematically sound checksum is created to maintain authenticity of disk image.
- Label and maintain Chain-of-Custody for the original evidence and all images.
- The imaged drive will become your working evidence. It is from here that you should perform all examinations and analysis.

Evidence Examination

Evidence examination is the point where we seek to find out if there is any true evidence useful to law enforcement and the legal process. An art as much as a science, evidence examination procedures can be as varied as platforms and installations.

No matter what type of case you are working, once you have imaged the evidence drives, you can outline your procedures as follows:

1. Find out what you are looking for. You may need help to establish this question. If you are working with a legal team during the discovery process get involved early so you can ensure all the possible data sources are collected. This will change somewhat from case to case. In some cases you will be looking for graphic files, in others the information will reside in email and document files.
2. Create a system report. Some cases may require a detailed report as to the status of the system. Include items such as applications installed, directory structure, recent web sites visited, viruses, Trojans, etc.
3. Recover any deleted files and slack space from the media.
4. On system drives it is often helpful to delete known files such as system drivers, executables and support files. That is, of course, if you are only searching for data and not analyzing the performance and characteristics of the system. You may find it useful to create and maintain known file checksums to aid in this process.
5. Identify and decrypt any encrypted files.
6. Convert any file formats needed to prepare for searching and indexing. This step may include extracting email files.
7. Conduct Search.
8. Index results and prepare report for third party analysis.
9. Hash values should be created for files of interest.
10. Individual files may need to be organized and numbered as evidence if intended to be admitted into court.

There are many tools available and you will most likely use more than one to achieve the steps outlined above. Don't forget that authenticity can be questioned based on the applications utilized. The use of well known and professional software tools is a must. The Resources section of this document contains links to many well known and commonly used tools.

As in every step before, create extensive documentation of your examination process, as well as the results.

References

- Department of Justice Search & Seizure Manual dated January 2001 – Online at http://www.cybercrime.gov/searching.html#FED_GUID
- Computer Forensics Incident Response Essentials by Warren G. Kruse II and Jay G. Heiser. Published by Addison Wesley

- Handbook of Computer Crime Investigation - Forensic Tools and Technology by Eoghan Casey, et al. Published by Academic Press
- Computer Incident Response – Scott Grace - <http://www.sans.org/infosecFAQ/incident/IRCF.htm>

Agencies, Contacts & Resources

US Attorney's Office – <http://www.usDoJ.gov/ag/>

FBI Laboratory Computer Analysis and Response Team -
<http://www.fbi.gov/hq/lab/org/cart.htm>

DOJ Electronic Evidence Resource List -
http://www.ojp.usDoJ.gov/nij/cybercrime_resources.htm

NCIS Computer Crimes - <http://www.ncis.navy.mil/activities/CompCrim/CompCrim.html>

HTCIA (High Technology Computer Investigation Association) - <http://htcia.org/>

List of Technology Lawyers and Law Firms - <http://www.kuesterlaw.com/>

Computer Forensics Online Magazine - <http://www.shk-dplc.com/cfo/>

CyberCrime - <http://www.cybercrime.gov/>

Technology Pathways LLC – <http://www.TechPathways.com>

List Servers

Computer Forensics Tool Testing (cftt@yahoogroups.com)

This group is for discussing and coordinating computer forensics tool testing. Testing methodologies will be discussed, as well as, the results of testing various tools. The ultimate goal of these tests is to ensure that tools used by computer forensics examiners are providing accurate and complete results.

This discussion group is open to all individuals in the field who are interested in participating in the testing of computer forensics tools.

To learn more about the CFTT group, please visit <http://groups.yahoo.com/group/cftt>

Forensics (forensics@TechPathways.com)

Technology Pathways provides the Forensics discussion list as a means of support to the Computer Forensics community. This mailing list is a non-product specific list which should be used to discuss our tools and techniques, as well as, those of other vendors and consultants. The Technology Pathways staff does monitor the Forensics list, so you should find it a good adjunct for technical support.

To subscribe to the Forensics list send a blank email to: forensics-subscribe@TechPathways.com

To unsubscribe to the Forensics list send a blank email to: forensics-unsubscribe@TechPathways.com

For questions regarding this list, please email: listmaster@TechPathways.com

Forensics (forensics@securityfocus.com)

The FORENSICS mailing list is a discussion mailing list on the topic of technical and process methodologies for the application of computer forensics. The discussion is centered around such things as:

Technical Methodology for the Application of Computer Forensics. This is not system or software specific and is open for wide discussion. The discussion will be centered around such things as:

- Audit trail analysis. (Technical)
- General postmortem analysis. (Technical)
- Products and tools for use in this field. (Technical)

To learn more about the Forensics group, please visit <http://www.securityfocus.com/cgi-bin/forums.pl>

Appendix E: End-user License Agreement and Product Licensing

Software Licence and Copy Protection

Each copy of ProDiscover is licensed for one concurrent use and may be installed on up to three workstations. ProDiscover's software copy protection mechanism utilizes a alpha-numeric key to lock each copy of ProDiscover to a single workstation and will not allow it to function on workstations for which it is not licensed. Customers who require installing ProDiscover on more than one workstation or who need to move of ProDiscover to another workstation should contact Technology Pathways Support (support@TechPathways.com) for additional keys.

End-User License Agreement

PLEASE READ THIS LICENSE CAREFULLY BEFORE USING THIS SOFTWARE. ALL SECTIONS APPLY TO BOTH TRIAL LICENSES AND PURCHASED LICENSES EXCEPT THOSE SECTIONS FOR PERMITTED USES AND PROHIBITED USES. BY INSTALLING THIS SOFTWARE, YOU ACKNOWLEDGE THAT YOU HAVE READ THIS AGREEMENT, UNDERSTAND IT, AND AGREE TO BECOME BOUND BY ITS TERMS AND CONDITIONS.

Copyright & Proprietary Information. The enclosed software (the "Software") is the property of Technology Pathways, LLC ("Technology Pathways"). As copyrighted and trademarked material, it is protected by United States and international copyright and trademark laws and treaties, and international trade provisions. Your purchase or trial use of the disks or files containing the Software transfers no title to the Software itself. Instead, any use of such Software must be made in accordance with the terms of this License. Technology Pathways reserves all rights not specifically granted herein. Your rights and obligations under this License are set forth below. If you violate such obligations, this License and your right to use the Software terminate immediately.

Permitted Uses of a Trial License. Under this License, Technology Pathways grants you the right to use the Software and documentation without charge for a trial period of thirty (30) days, by which time you will have purchased the software and will continue to be bound by the terms of this agreement; or will have discontinued all use of the Software and destroyed it and all copies thereof, in which event all of your rights hereunder shall end.

Prohibited Uses of a Trial License. You may not, and you may not authorize anyone else to (i) sell, rent, lend, assign, sublicense or transfer the Software or your rights hereunder except as expressly provided in this License; (ii) reverse engineer, disassemble, decompile, or make any attempt to discover the source code of the Software; or (iii) to make any copy of all or a part of the Software other than one copy (including all copyright, trademark and proprietary rights notices thereon) for backup purposes only and such copy shall constitute "Software" under this License.

Permitted Uses of a Purchased License. Under this License, Technology Pathways grants you the right to (i) install the Software (except for the PDSEVER Remote Agent) on a maximum of three computers for your internal business purposes only, however, only one copy may be used at any given time. Technology Pathways may allow the Software installation to be moved after initial installation. If the Software you purchased includes the PDSEVER Remote Agent, Technology Pathways grants you the right to use the PDSEVER Remote Agent on an unlimited number of computers; (ii) make one copy of the Software (including all copyright, trademark and proprietary rights notices thereon) for backup purposes only and such copy shall constitute "Software" under this License; and (iii) transfer the Software and documentation, including a copy of this License, to another person who agrees to become bound by the terms and conditions of this License and notifies Technology Pathways in writing of the transfer, in which event all of your rights hereunder shall end.

Prohibited Uses of a Purchased License. You may not, and you may not authorize anyone else (i) to operate the Software or any copy thereof on more than one computer at any time; (ii) to sell, rent, lend, assign, sublicense or transfer the Software or your rights hereunder except as expressly provided in this License; (iii) to electronically transfer the Software from one computer to another (unless you obtain

licenses from Technology Pathways for each of the machines using the Software); (iv) to reverse engineer, disassemble, decompile, or make any attempt to discover the source code of the Software; or (v) to make any copy of all or a part of the Software other than the one backup copy permitted above.

Termination. You may terminate this License at any time by discontinuing all use of the Software and destroying it and all copies thereof.

Limited Warranty & Limitations on Warranty

Limited Warranty and Liability. When the Software is furnished on diskettes, Technology Pathways warrants the disks to be free from defects in materials and workmanship under normal use for a period of sixty (60) days from the date of delivery to you as evidenced by your completed and returned registration card, which must be returned to Technology Pathways within ten (10) days of opening the disk package. Any replacement software will be warranted for the rest of the sixty (60) day period or for thirty (30) days from the date you receive the replacement, whichever is longer. Technology Pathway's entire liability and your exclusive remedy shall be, at Technology Pathway's option, either (a) to return the price paid or (b) to repair or replace the Software. This Limited Warranty is void if failure of the Software has resulted from accident, abuse, or misapplication.

Disclaimer of Warranties. THE SOFTWARE AND ASSOCIATED DOCUMENTATION ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY WARRANTY OF MERCHANTABILITY, FITNESS FOR ANY PARTICULAR PURPOSE, OR NON-INFRINGEMENT. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE SOFTWARE AND DOCUMENTATION IS WITH YOU. TECHNOLOGY PATHWAYS DOES NOT WARRANT THAT THE SOFTWARE WILL MEET YOUR REQUIREMENTS OR THAT THE OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR FREE, OR THAT DEFECTS IN THE SOFTWARE WILL BE CORRECTED. SOME STATES DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO THE ABOVE EXCLUSION MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, AND YOU MAY ALSO HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE.

Limitations of Warranty. IN NO EVENT SHALL TECHNOLOGY PATHWAYS OR ANY SUPPLIER OR ANY OTHER PERSON INVOLVED IN THE CREATION, PRODUCTION, OR DISTRIBUTION OF THE SOFTWARE BE LIABLE TO YOU ON ACCOUNT OF ANY CLAIM FOR ANY SPECIAL EXEMPLARY OR PUNITIVE DAMAGES, INCLUDING ANY LOST PROFITS, LOST SAVINGS, BUSINESS INTERRUPTION, LOSS OF BUSINESS OR PERSONAL INFORMATION OR ANY OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE, THE INABILITY TO USE, QUALITY, OR PERFORMANCE OF THE TECHNOLOGY PATHWAYS SOFTWARE AND DOCUMENTATION, EVEN IF TECHNOLOGY PATHWAYS, OR AN AUTHORIZED REPRESENTATIVE OF TECHNOLOGY PATHWAYS, HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. BECAUSE SOME STATES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATIONS MAY NOT APPLY TO YOU.

Government End Users. The Software and any associated documentation are provided with RESTRICTED RIGHTS. Use, duplication or disclosure by the Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of The Rights In Technical Data and Computer Software Clause at 52.227-7013.

General. All updates or new versions of the Software which may be received by you from Technology Pathways shall also be governed by this License. This License Agreement shall be construed, interpreted and governed by the laws of the State of California. If any provision of this License is found void or unenforceable, it will not affect the validity of the rest of this License. You may not export or re-export the Software except in compliance with the Export Administration Regulations of the U.S. Department of Commerce. Headings and captions are for convenience only and are not to be used in the interpretation of this Agreement.

Index

Action Menu	14	Create report thumbnails	128
Action Menu Commands	118	Creating a Linux PDServer Disk.....	66
Activating.....	4	Creating a PDServer Disk	65
Add Capture & Add Image.....	98, 120	Creating a PDServer Linux Boot Disk	66
Add Disk	99, 121	Creating and Running the Sun Remote Agent	65
Add Image	98, 120	Creating Hash Database Files	46
Add an image file to a project.....	26	Cross Reference File Cluster Locations.....	56
Batch Calculate Hashing	137	Customizing.....	7
Bates Numbering	136	Data View Area	11
BIOS Imaging	120	Detecting Installed OS	54
Boolean Logic	44	Disconnect.....	116
Boolean search	149	Disk	65
Button Bar.....	13	Disk Groups and Dynamic Disks	118
Capture an image of an attached drive	21	Disk Inventory	127
Capture Image	118	Encryption	117
Capturing Physical Memory	22	EventLog Viewer	103
CD-ROM	65	Evidence Examination	161
Clear Recent Projects List	125	Evidence of Interest	
Clear Report All.....	125	Adding Comments.....	60
Clear Report Clusters of Interest	125	Adding Subsets of Data	61
Clear Report Evidence of Interest	124	EXIF Meta Data	40
Clear Report File Signature Mismatch.....	124	Exit	115
Clear Report OS Info	124	Export.....	126
Clear Report Ports List.....	125	Export Evidence of Interest.....	128
Clear Report Process List	125	Extracting Internet History	45
Clear Report Registry Keys of Interest.....	125	File Menu.....	14
Clear Report Search Results.....	124	File Menu Commands	108
Clear Report System State.....	125	Filter by Hash Set	137
Clear Report Unseen Processes.....	125	Find Suspect Files	144
Cluster View.....	101, 130	Find Unseen Files	141
Cluster View of Drive Partition	103, 131	Find Unseen Processes	141
Cluster View of Physical Drive.....	102, 130	Flagging or Bookmarking Evidence of Interest.....	58
Compare Baseline	144	Floppy Disk	65
Compress	125	Gallery View.....	132
Computer Shutdown	160	Get Process List.....	146
Conducting Live Preview of a Remote Disk	20	Get System State.....	146
Connect To	116	Hardware Protected Area	50
Content View Disk	101, 130	HashKeeper hash sets	47
Content View Image.....	101, 129	Help	9
Convert "DD" Image to "ISO"	140	Help Menu	16
Convert ProDiscover Image to "DD"...	139	Image Conversion Tools	138
Convert ProDiscover Image to "ISO"	140	Imaging Evidence Drives.....	160
Convert Project Format	140	Installing ProDiscover	3
Copy	30	Internet History Viewer	104
Copy Disk.....	135	IR Menu	16
Copy Selected Clusters.....	136	IR Menu Commands	141
Copy Selected Files.....	31, 135	License	163
Create Baseline	143	Maintain Chain of Custody.....	160
Create remote server disk	140	Match File Signatures.....	49

Network Imaging & Analysis of Live Systems	63	Search	43, 105
Network Menu	14, 116, 117	Search –	122
Network Menu Commands	116	Search The Windows Registry	35
New Project	17, 108	Secure Wipe	135
Open Image	108	Server	65
Open Project	108	Signature Matching	137
Open/Connected IP Ports	148	Starting	5
OS Info	127	Startup Dialog	132
PDServer	65	Status Bar	132
PDServer Command Line Options	68	Stealth Mode	66
PDServer Remote Agent Firewall		Stop Search	124
Configuration	70	System requirements	3
PDServer™ Remote Installation and		Technical Support	III
Removal Scripts	72	Thumbnail Images	40
Perl	89	Tool Bar	132
Physical Memory	120	Tools Menu	15
Preferences	7, 109	Tools Menu Commands	135
Print Report	115	Tree View Area	12
Print Setup	114	Tree View Commands	97
ProDiscover Features	6	Tree-View Items	12
ProScript	89	Troubleshooting PDServer Connection	
ProScript API	89	Problems	75
Recover a Deleted File	42	UnCompress	126
Recover a group of clusters	53	UNIX "dd" image	28
Registry Viewer	103	USB Flash Disk	65
Release Remote Client	117	Using ProDiscover	
Remote Agent	63	Basics	7
Remove	100	Using the PDServer Linux Boot Disk	69
Report	97, 129	Verify Image Checksum	127
Restore	31	View Log	104
Run	65	View Log File	132
Windows	65	View Menu	15
Save a Project	17	View Menu Commands	129
Save As	108	View Windows Registry	33
Save Project	108	Viewing Graphic Files in Gallery View	39
Scan HPA	138	VMWare Support for "DD" Images ...	140